UCH UNIVERSIDAD DE CIENCIAS Y HUMANIDADES

FACULTAD DE CIENCIAS E INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabif

PRESENTADO POR

Castillo Porturas, Augusto Noé

ASESOR

Andrade Arenas, Laberiano Matías

Los Olivos, 2015

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

IMPLEMENTACIÓN DE REDES VIRTUALES UTILIZANDO VLAN PARA REDUCIR EL TAMAÑO DEL DOMINIO DE DIFUSIÓNDE LA RED EN EL INABIF

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMATICA

PRESENTADO POR:

CASTILLO PORTURAS, AUGUSTO NOÉ

ASESOR:

ANDRADE ARENAS, LABERIANO MATÍAS

LIMA - PERÚ

2015

SUSTENTADO Y APROBADO POR LOS SIGUIENTES JURADOS:

_____	_____
JURADO 1	JURADO 2
JESUS VILCHEZ	JUAN VASQUEZ
SANDOVAL	PARAGULLA
PRESIDENTE	SECRETARIO
_____	_____
JURADO 3	ASESOR
ULISES LAPA	LABERIANO ANDRADE
ASTO	ARENAS
VOCAL	**ASESOR**

DEDICATORIA.

A mis padres Ignacio y Consuelo,

por su permanente aliento,

guía y apoyo incondicional.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

El presente es testigo de una novedosa forma de comunicación en un entorno globalizado debido a la expansión y desarrollo de la Internet. Por esta razón, se ha hecho indispensable dentro de las organizaciones el mejoramiento de las infraestructuras tecnológicas, tanto en la red convencional como en la red inalámbrica. Sin embargo, muchas instituciones del Perú, especialmente las estatales, no toman en cuenta que sus infraestructuras, tal como se encuentran, dificultan su óptimo funcionamiento; por lo que es necesario implementar redes virtuales que permitan viabilizar mejor la comunicación y proteger la información, de posibles filtraciones de usuarios ajenos al área específica, lo cual podría generar pérdidas financieras o espionaje corporativo. Para evitar esto se cuenta con estándares y metodologías que permiten constituir soluciones prácticas.

En el primer capítulo se planteó un estudio del problema ubicándole en el escenario real para poder especificar las necesidades de la institución, la cual requiere una solución mediante redes virtuales que garanticen el uso adecuado de la red.

En el segundo capítulo se establecen los objetivos los que se debe alcanzar con esta investigación.

En el tercer capítulo se hace una exposición del por qué es justo para el INABIF diseñar e implementar redes virtuales en su sistema de red actual.
En el cuarto capítulo se menciona los alcances que tendrá este proyecto, pues el INABIF es una entidad con filiales en Lima entre **CAR** (Centro de Atención Residencial) **y CEDIF** (Centro de Desarrollo Integral de la Familia).

En el quinto capítulo se explora por el marco teórico referente al tema que es muy amplio; pero se ha considerado solamente lo más próximo y afín a nuestro tema de estudio.

Las redes virtuales implementadas serán útiles para reducir el tamaño del dominio de difusión y ayudarán a la administración de la red separando en segmentos lógicos de la red que involucra las diversas áreas del INABIF

Con esta reestructuración de la red en la institución se logrará que la productividad del usuario y la adaptabilidad de la red sean impulsores clave para el crecimiento y el éxito del negocio. La implementación de esta tecnología va permitir que una red admita de manera más flexible las metas comerciales. Los principales beneficios de usar VLAN son los siguientes: seguridad de grupos de trabajo y de red, reducción de costes administrativos relacionados con la solución de los problemas asociados con los traslados, adiciones y cambios, mejor rendimiento, mitigación de la tormenta de broadcast, mayor eficiencia del personal de TI y la administración de proyectos más simples.

CAPÍTULO I: ASPECTOS GENERALES

1.1 DEFINICIÓN DEL PROBLEMA.

Descripción del problema.

La red actual está diseñada con 9 gabinetes en los que hay switches, enlaces de datos y enlaces de voz (no es voip). Los dispositivos con lo que se cuenta son: 3 Firewall, 1 Router del ISP (Claro), 8 switch, 320 Pcs, 1 dominio www.inabif.gob.pe, 2 servidores de dominio, el proveedor de Internet es Claro de tipo **Dedicado** (Ancho de banda real 12MB)

Esta red física implica que el tamaño del dominio de difusión sea muy grande por endelos datos estén siendo intercambiados indiscriminadamente en todos los departamentos y áreas de la entidad.

El INABIF es dependencia del MIMDES (Ministerio de la Mujer y Poblaciones Vulnerables) y como es sabido, las instituciones del estado por lo general no están a la vanguardia de la tecnología. Por diversos motivos como por presupuesto o por cuestiones netamente políticas. Tenemos conocimiento de que la misma entidad matriz tiene muchas carencias en su área de sistemas en general y siendo un punto vulnerable su sistema de red existente. Esto es una preocupación porque se entiende que el problema se suscita aún por el descuido en las instancias superiores. Aún cuando las instancias inferiores luchen por sobrellevar las tareas encomendadas, sobreponiéndose a las dificultades que generan estos desaciertos en la tecnología existente, no llegarán a más si no se implanta una solución práctica y sólida en su concepto.

Como algunas dificultades específicas se puede mencionar a: los servidores muy antiguos, lentitud de acceso a la red cuando se inicia la sesión, mal

dimensionamiento del cableado estructurado, en ciertos tramos el cableado comparte el mismo tendido con la corriente eléctrica, el acceso indiscriminado a la información de diferentes áreas, la distribución inadecuada del ancho de banda.

Estamos ante una institución no pequeña, si no de gran magnitud, con dependencias, a su vez, en provincia; por ende, los problemas que genera tener una sola red física repercuten en las dependencias del interior también. La cantidad de información que se maneja es grande por ser de una entidad nacional, esto hace la demanda de soluciones prontas.

Formulación del problema.

¿La implementación de redes virtuales utilizando Vlan permitirá reducir el tamaño del dominio de difusión de la red en el INABIF?

FORMULACIÓN DE LOS PROBLEMAS ESPECÍFICOS.

Formulación del problema específico 1:

¿La implementación de redes virtuales permitirá el control de ancho de banda encada área de la institución?

Formulación del problema específico 2:

¿La implementación de redes virtuales brindará mayor seguridad en el tráfico y acceso de la información que viaja por la red de la institución?

1.2 DEFINICIÓN DE LOS OBJETIVOS DE LA INVESTIGACIÓN.

Objetivo general.

Reducir el tamaño del dominio de difusión de la red en el INABIF.

Objetivos específicos.

Objetivo específico 1: Controlar el ancho de banda en cada aérea de la institución.

Objetivo específico 2: Brindar mayor seguridad en el tráfico y acceso de la información que viaja por la red de la institución.

1.3 DE LA INVESTIGACIÓN.

En lo económico, la implementación de este proyecto significará ahorro; pues éste resultaría de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.

En lo operativo, la división de redes planas de capa 2 en múltiples grupos lógicos de trabajo (dominio de broadcast) reducirá el tráfico innecesario en la red y potenciará el rendimiento.

En lo tecnológico, con este proyecto se dará un uso más eficiente de los equipos ya existentes dentro de la institución, disminuyendo la capacidad ociosa de los mismos. Está innovación será propulsora de mayores rendimientos y beneficios para la productividad, logrando así cubrir la demanda actual.

En lo institucional, con esta implementación se generará mejoras en las condiciones de trabajo para técnicos, profesionales y usuarios en general. Por lo tanto entre los trabajadores más relacionados al tema se vivirá un mejor clima laboral y para los usuarios externos habrá una mejoría en las atenciones y servicios.

1.4 ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN.

ALCANCES.

Este proyecto tiene alcance a nivel de todas las dependencias de Lima, podría también ser a nivel nacional, pero las dependencias del interior del país manejan sus presupuestos de manera independiente. Más aún se podría crear una VPN, que es una tecnología de red que permite una extensión de la red local sobre una red pública no controlada.

Esta investigación también podrá servir como base para aplicar sus resultados a otras instituciones del estado o privadas con manejo administrativo de datos similares, puesto que el modelo VLAN es de variada aplicación en la actualidad.

Los trabajadores de la entidad serán partícipes de la implementación y manejo de esta nueva tecnología, ampliando sus conocimientos e incentivando a trabajar en busca de mejoras en otros aspectos del área de sistemas o de otras áreas relacionadas al tema.

LIMITACIONES.

Ya que es un tema particular de las telecomunicaciones es muy importante la experiencia en el manejo de esta tecnología.

Para realizar un certero diagnóstico del problema se necesita acceso a la infraestructura de red. Aspectos como la política de una institución estatal, las formalidades y burocracia se convierten en restricciones para la investigación y no facilitan el trabajo.

La Deficiente tecnología en la infraestructura de red del INABIF, no ayuda a identificar con plenitud las deficiencias cotidianas en la red.

La implementación de Vlans genera desconfianza en algunos técnicos acostumbrados y mecanizados a su vieja tecnología, adicionalmente sería muy adecuado organizar una charla con los trabajadores que se verán afectados por esto, pero aun eso es casi imposible por políticas de la institución.

CAPITULO II: FUNDAMENTO TEÓRICO

2.1 ANTECEDENTES

- Tipán Lema, Milton Santiago, (2005), **"Implementación de Vlans en la red de Telconet para una interconexión segura entre las agencias y la matriz de una institución bancaria"**

  Telconet asume la necesidad y presenta una alternativa basada en VLANS, esta solución cubre las necesidades del banco tanto en el aspecto funcional como en el aspecto relacionado a los costos, ya que el valor de los enlaces dedicados provistos por Telconet a la Institución Bancaria están acorde al mercado actual de las comunicaciones.

- Molina Ruiz, Julio Edgard, (2012), **"Propuesta de Segmentación con Redes Virtuales y Priorización del Ancho De Banda con Qos para la mejora del Rendimiento y Seguridad de la Red Lan en la Empresa Editora El Comercio Planta Norte."**

  Este proyecto se realiza para segmentar las áreas en subredes para un mayor nivel de protección: brindar seguridad (Listas de Control de Acceso ACL's. Tecnologías emergentes en seguridad Windows Server 2008. Nivel de autentificación - Radius); mejorar el consumo de Ancho de Banda (Calidad de Servicio QoS. Protocolos de agregación de enlaces de control LACP. Troncales, etc.); implementar nuevos protocolos en tecnologías CISCO: instalar redes inalámbricas y nuevos Servicios de transferencia de Archivos (Protocolos de Transferencia de Archivos FTP)

- Tigre Cortés, Jonathan Javier, (2012) **"Diseñar el desarrollo de redes Virtuales Locales (VLAN) para aislar el tráfico de broadcast"**

Se ha realizado el diseño y la configuración de las VLAN, para solucionar el problema que tienen las redes LAN dentro de las empresas de Cuenca para aislar el tráfico de los dominios de broadcast dentro de una red conmutada. Segmentando la red en VLAN , para mejorar la administración de la red separando el tráfico de datos, administración y voz a través de un nombre común para poder identificarlas dentro de la red. Para evitar el tráfico de broadcast utilizamos el método basado en puerto que nos ayuda evitar que las tramas de broadcast se propaguen por toda la red. Utilizamos un router para la comunicación entre VLAN y controlar los dominios de broadcast.

2.2 MARCO TEÓRICO

HARDWARE DE REDES

Es tiempo de centrar nuevamente la atención en los temas técnicos correspondientes al diseño de redes (la parte del trabajo) y dejar a un lado las aplicaciones y los aspectos sociales de la conectividad (la parte divertida). Por lo general, no hay una sola clasificación aceptada en la que se ajusten todas las redes de computadoras, pero hay dos que destacan de manera importante: la tecnología de transmisión y la escala.

En un sentido amplio, hay dos tipos de tecnología de transmisión que se utilizan de manera extensa. Son las siguientes:

- Enlace de difusión
- Enlace de punto a punto.

Las **Redes de difusión** (broadcast) tienen un solo canal de comunicación por lo que todas las máquinas de la red lo comparten. Si una máquina envía un mensaje corto –en ciertos contextos conocido como **paquete**-, todas las demás lo reciben. Un campo de dirección dentro del paquete especifica el destinatario. Cuando una máquina recibe un paquete, verifica el campo de dirección. Si el paquete va direccionado a esa máquina, ésta lo procesa; si va destinado a alguna otra, lo ignora.

En contraste, las **Redes punto a punto** constan de muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red podría tener que visitar primero una o más máquinas intermedias. A menudo es posible que haya varias rutas o longitudes diferentes, de manera que encontrar las correctas es importante en redes de punto a punto. Por regla general (aunque hay muchas excepciones), las redes más pequeñas localizadas en una misma área geográfica tienden a utilizar la difusión, mientras que las más grandes suelen ser de punto a punto con un emisor y un receptor se conoce como **unidifusión** (unicasting)

REDES DE AREA LOCAL.

Las **redes de área local** (generalmente conocidas como LANs) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras

personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información. Las LANs son diferentes de otros tipos de redes en tres aspectos: 1) tamaño; 2) tecnología de transmisión; y 3) topología.

Las LANs están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño, lo cual no sería posible de otra manera. Esto también simplifica la administración de la red[1].

REDES DE AREA METROPOLITANA.

Una **red de área metropolitana** (MAN) abarca una ciudad. El ejemplo más conocido de una MAN es La red de televisión por cable disponible en muchas ciudades. Este sistema creció a partir de los primeros sistemas de antena comunitaria en áreas donde la recepción de la televisión al aire era pobre. En dichos sistemas se colocaba una antena grande en la cima de una colina cercana y la señal se canalizaba a las casas de los suscriptores.

Al principio era sistemas diseñados de manera local con fines específicos. Después las compañías empezaron a pasar a los negocios, y obtuvieron contratos de los gobiernos para cablear toda una ciudad. El siguiente paso fue la programación de la televisión e incluso canales designados únicamente para cable. Con frecuencia estos emitían programas de un solo tema, como solo

[1] Andrew S. Tanenbaum, 2003, Redes de Computadoras, Pagina 16.

noticias, deportes, cocina, jardinería, etc. sin embargo desde su inicio y hasta finales de la década de 1990, estaban diseñados únicamente para la recepción de televisión.

A partir de que Internet atrajo una audiencia masiva, los operadores de la red de TV por cable se dieron cuenta de que con algunos cambios al sistema, podrían proporcionar servicio de Internet de dos vías en las partes sin el uso del espectro. En ese punto, el sistema de TV por cable empezaba a transformarse de una forma de distribución de televisión a una red de área metropolitana[2].

REDES DE ÁREA AMPLIA.

Una **red de área amplia** (WAN), abarca una gran área geográfica, con frecuencia un país o un continente. Contiene un conjunto de máquinas diseñado para programas (es decir, aplicaciones) de usuario. Seguiremos el uso tradicional y llamaremos **hosts** a estas máquinas. Los hosts están conectados por una **subred de comunicación,** o simplemente **subred,** para abreviar. Los clientes son quienes poseen a los hosts (es decir, las computadoras personales de los usuarios), mientras que, por lo general, las compañías telefónicas o los proveedores de servicios de Internet poseen y operan la subred de comunicación. La función de una subred es la de llevar un mensaje de un host a otro, como lo hace el sistema telefónico con las palabras del que habla al que escucha. La separación de los aspectos de la comunicación pura de la red (la subred) de los

[2] Andrew S. Tanenbaum, 2003, Redes de Computadoras, Pagina 18.

aspectos de la aplicación (los hosts), simplifica en gran medida todo el diseño de la red[3].

REDES INALÁMBRICAS.

La comunicación inalámbrica digital no es una idea nueva. A principios de 1901, el físico italiano Guillermo Marconi demostró un telégrafo inalámbrico desde un barco a tierra utilizando el código Morse (después de todo los, los puntos y rayas son binarios). Los sistemas inalámbricos digitales de la actualidad tienen un mejor desempeño, pero la idea básica es la misma.

Como primera aproximación, las redes inalámbricas se pueden dividir en tres categorías principales:

Interconexión de sistemas.

LANs inalámbricas.

WANs inalámbricas.

SOFTWARE DE REDES

REDES DE EJEMPLO

El tema de las redes de computadoras cubre muchos y diversos tipos de redes, grandes y pequeñas, bien conocidas y no tan bien conocidas. Tiene diferentes

[3] Andrew S. Tanenbaum, 2003, Redes de Computadoras, Pagina 19.

objetivos, escalamientos y tecnologías. En las siguientes secciones veremos algunos ejemplos para tener una idea de la variedad que se puede encontrar en el área de la conectividad de redes.

INTERNET.

Internet no es del todo una red, sino un inmenso conjunto de redes diferentes que usan ciertos protocolos comunes y proporcionan ciertos servicios comunes. Es un sistema poco común porque nadie lo planeó y nadie lo controla. Para entenderlo mejor, empecemos desde el principio y veamos cómo se desarrolló y por qué. Si desea leer una historia maravillosa sobre Internet, recomendamos ampliamente el libro de Llano (1993). Es uno de esos raros libros cuya lectura no sólo es divertida, sino que también contiene 20 páginas de *ibídems*y*op. cits*. para el historiador serio.

ARPANET. Nuestro relato empieza a fines de la década de 1950. Durante el auge de la Guerra Fría, el DoD quería una red de control y comando que pudiera sobrevivir a una guerra nuclear. En esa época todas las comunicaciones militares usaban la red telefónica pública, que se consideraba vulnerable. La razón de esta creencia se puede entresacar de la figura 1-25(a). Hacia 1960, el DoD(UbitedStatesDepartament of Defense) firmó un contrato con RAND Corporation para encontrar una solución. Uno de sus empleados, Paul Baran, presentó el diseño de amplia distribución y tolerancia a fallas que se muestra en la figura 1-25(b). Puesto que las trayectorias entre cualquiera de las oficinas de conmutación eran ahora más grandes de lo que las señales análogas podían

viajar sin distorsión, Baran propuso que se utilizara la tecnología digital de conmutación de paquetes a través del sistema.

Cuando el presidente Eisenhower trató de encontrar quién estaba dormido en sus laureles, se espantó al encontrarse con que la armada, el ejército y la fuerza aérea se peleaban por el presupuesto de investigación del Pentágono. Su respuesta inmediata fue crear una organización única de investigación para la defensa, **ARPA** (**Agencia de Proyectos de Investigación Avanzada**)**.** Ésta no tenía científicos ni laboratorios; de hecho, no tenía más que una oficina y un presupuesto pequeño (por normas del Pentágono). Hacía su trabajo otorgando subvenciones y contratos a universidades y empresas cuyas ideas le parecían prometedoras.

Durante los primeros años, ARPA trataba de imaginarse cuál sería su misión, pero en 1967 la atención de su entonces director, Larry Roberts, se volvió hacia las redes. Se puso en contacto con varios expertos para decidir qué hacer. Uno de ellos, Wesley Clark, sugirió la construcción de una subred de conmutación de paquetes, dando a cada *host* su propio enrutador.

NSFNET. A finales de la década de 1970, la NFS (Fundación Nacional para las Ciencias, de Estados Unidos) vio el enorme impacto que ARPANET estaba teniendo en la investigación universitaria, permitiendo que científicos de todo el país compartieran datos y colaboraran en proyectos de investigación. Sin embargo, para estar en ARPANET, una universidad debía tener un contrato de investigación con el DoD, lo cual muchas no tenían. La respuesta de la NSF fue diseñar un sucesor de ARPANET que pudiera estar abierto a todos los grupos de investigación de las universidades. Para tener algo concreto con que empezar, la

NSF decidió construir una red dorsal (o troncal) para conectar sus seis centros de supercomputadoras en San Diego, Boulder, Champaign, Pittsburgh, Ithaca y Princeton. A cada supercomputadora se le dio un hermano menor, que consistía en una microcomputadora LSI-11 llamada ***fuzzball***. Estas computadoras estaban conectadas a líneas alquiladas de 56 kbps y formaban una subred, utilizando la misma tecnología de hardware que ARPANET. Sin embargo, la tecnología de software era diferente: las *fuzzball*utilizan TCP/IP desde el inicio, creando así la primera WAN TCP/IP.

La NSF también fundó algunas redes regionales (alrededor de 20) que se conectaban a la red dorsal para que los usuarios en miles de universidades, laboratorios de investigación, bibliotecas y museos, tuvieran acceso a cualquiera de las supercomputadoras y se comunicaran entre sí. Toda la red, incluyendo la red dorsal y las redes regionales, se llamó **NSFNET.** Ésta se conectó aARPANET a través de un enlace entre un IMP y una *fuzzball*en el cuarto de máquinas de Carnegie-Mellon. En la figura 1-28 se muestra la primera red dorsal NSFNET.

Uso de Internet.

El número de redes, máquinas y usuarios conectados a ARPANET creció rápidamente luego de que TCP/IP se convirtió en el protocolo oficial el 1o. de enero de 1983. Cuando NSFNET y ARPANET estaban interconectadas, el crecimiento se hizo exponencial. Muchas redes regionales se unieron y se hicieron conexiones a redes en Canadá, Europa y el Pacífico.

En algún momento a mediados de la década de 1980, las personas empezaron a ver el conjunto de redes como una interred y más tarde como Internet, aunque no

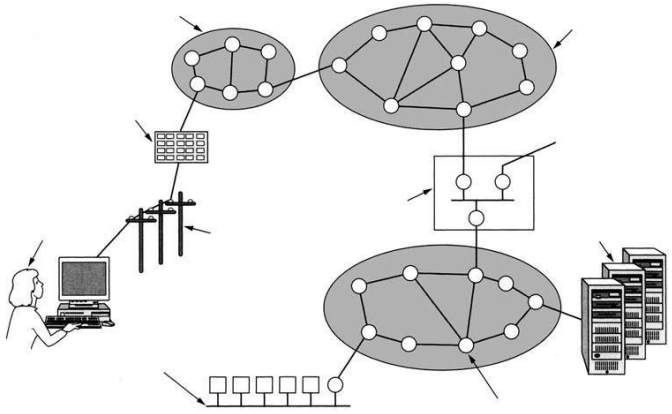
hubo una inauguración oficial con algún político rompiendo una botella de champaña sobre una *fuzzball*.

El aglutinante que mantiene unida la Internet es el modelo de referencia TCP/IP y la pila de protocolos de TCP/IP. TCP/IP hace posible el servicio universal y se puede comparar con la adopción de la medida estándar para el ancho de vía del ferrocarril en el siglo XIX o la adopción de los protocolos de señalización comunes para las compañías telefónicas.

Tradicionalmente (es decir, de 1970 a 1990) Internet y sus predecesores tenían cuatro aplicaciones principales: **correo electrónico, noticias, inicio remoto de sesión, transferencia de archivos.**

Hasta principios de la década de 1990, Internet era muy visitada por investigadores académicos, del gobierno e industriales. Una nueva aplicación, **WWW** (**World Wide Web**) cambió todo eso y trajo millones de usuarios nuevos no académicos a la red[4].

Figura 1.1: Panorama del Internet



FUENTE: Libro Redes de Computadoras Andrew S Tanenbaum

[4] Andrew S. Tanenbaum, 2003, Redes de Computadoras, Pagina 57.

REDES ORIENTADAS A LAS CONEXIONES: X.25, FrameRelay, y ATM.

X.25 Y FrameRelay. Nuestro primer ejemplo de red orientada a la conexión es la **X.25,** que fue la primera red de datos pública. Se desplegó en la década de 1970, cuando el servicio telefónico era un monopolio en todas partes y la compañía telefónica de cada país esperaba que hubiera una red de datos por país —la propia. Para utilizar X.25, una computadora establecía primero una conexión con la computadora remota, es decir, hacía una llamada telefónica.

Circuitos Virtuales ATM. Puesto que las redes ATM están orientadas a la conexión, el envío de datos requiere que primero se envíe un paquete para establecer la conexión. Conforme el mensaje de establecimiento sigue su camino a través de la subred, todos los conmutadores que se encuentran en la ruta crean una entrada en sus tablas internas tomando nota de la existencia de la conexión y reservando cuales quiere cursos que necesite la conexión. Con frecuencia a las conexiones se les conoce como **circuitos virtuales,** en analogía con los circuitos físicos utilizados en el sistema telefónico. La mayoría de las redes ATM soportan también **circuitos virtuales permanentes,** que son conexiones permanentes entre dos *hosts* (distantes).

ETHERNET.

La historia empieza en la prístina Hawái a principios de la década de 1970. En este caso,“prístina” se puede interpretar como “que no tiene un sistema telefónico

funcional". En tanto los días son más agradables para los vacacionistas cuando no son interrumpidos por el teléfono, no fue así para el investigador Norman Abramson y sus colegas de la Universidad de Hawaii, quienes estuvieron tratando de conectar usuarios de las islas remotas a la computadora principal de Honolulu. Conectar sus propios cables bajo el Océano Pacífico parecía imposible, de modo que buscaron una solución diferente.

La primera que encontraron fueron los radios de onda corta. Cada terminal estaba equipada con un radio pequeño de dos frecuencias: un canal ascendente (a la computadora central) y otro descendente (desde la computadora central). Cuando el usuario deseaba conectarse con la computadora, sólo transmitía por el canal ascendente un paquete que contenía los datos. Si en ese instante nadie más estaba transmitiendo, probablemente el paquete saldría y su recepción sería confirma da en el canal descendente.

LANs INALÁMBRICAS: 802.11

Casi al mismo tiempo que aparecieron las computadoras portátiles, muchas personas tuvieron el sueño de andar por la oficina y poder conectar a Internet su computadora. En consecuencia, varios grupos empezaron a trabajar para cumplir con esta meta. El método más práctico es equiparlas computadoras de la oficina y las portátiles con transmisores y receptores de radio de onda corta que les permitan comunicarse. Este trabajo condujo rápidamente a que varias empresas empezaran a comercializar las LANs inalámbricas.

El problema es que no había compatibilidad entre ninguna de ellas. Esta proliferación de estándares implicaba que una computadora equipada con un

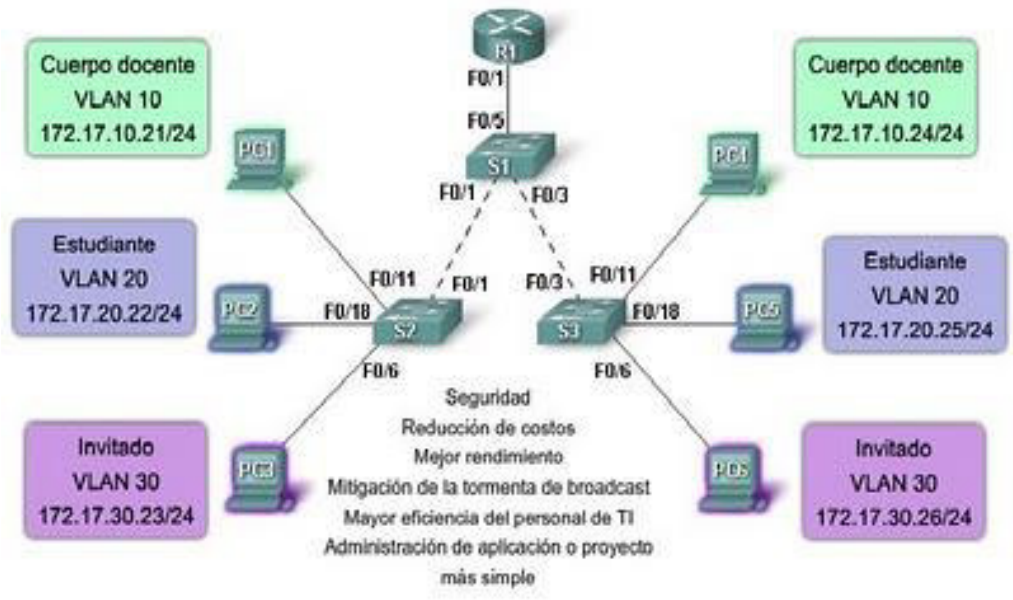
radio de marca *X* no funcionara en un cuarto equipado con una estación de base marca *Y*. Finalmente, la industria decidió que un estándar de LAN inalámbrica sería una buena idea, por lo que al comité del IEEE que estandarizó las LANs alámbricas se le encargó la tarea de diseñar un estándar para LANs inalámbricas. El estándar resultante se llamó 802.11. En la jerga común se le conoce como **WiFi.** Es un estándar importante y merece respeto, así que lo llamaremos por su nombre propio, 802.11.

DEFINICIÓN DE VLAN.

Las LANs virtuales (VLANs) son agrupaciones, definidas por software, de estaciones LAN que se comunican entre si como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de comunicación LAN se están introduciendo a este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios[5].

[5] http://polaris.lcc.uma.es/-eat/services/rvirtual/rvirtual.html#link 1

Figura 1.2:Ejemplo de Vlan



Fuente: https://www.google.com.pe/search?gs_rn=25&gs_ri=psy-ab&tok=WVJ1zmY-NY5RdRwqK8dhVA&cp=4&gs_id=q&xhr=t&q=nsfnet&bav=on.2,or.r

¿Qué hacen las redes virtuales (VLANs)? Una red virtual es un dominio de brodcast, es decir, cada VLAN tiene su propio dominio de brodcast. Como en un concentrador, todos los dispositivos en una red virtual ve todos los brodcasts así como también todas las tramas con dirección de destino desconocida, sólo que los brodcast y tramas desconocidas son originales dentro de esta red virtual.

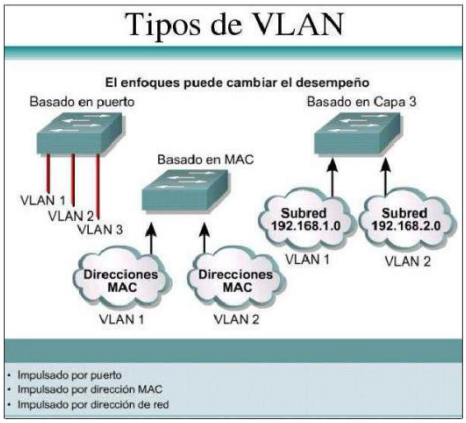
Además, la red virtual simplifica el problema de administrar los movimientos, adicionales y cambios de usuario dentro de la empresa. Por ejemplo, si un departamento se desplaza a un edificio a través del campus, este cambio físico será transparente gracias a la visión lógica de la red virtual. Así mismo, se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica al coste de unas pocas pulsaciones del ratón del administrador de la red. Puesto que todos los cambios

de la red. Puesto que todos los cambios se realizan bajo control de software, los centros de cableado permanecen seguros y a salvo de interrupciones[6].

Existen tres métodos principales de definición de pertenencia a VLAN:

- VLAN por puerto.
- VLAN por dirección MAC.
- VLAN por filtros.

Figura 1.3: Tipos de Vlan



FUENTE: https://www.google.com.pe/search?gs_rn=25&gs_ri=psy-ab&tok=WVJ1zmY-NY5RdRwqK8dhVA&cp=4&gs_id=q&xhr=t&q=nsfnet&bav=on.2,or.r_c

VLAN POR PUERTO

También llamada VLAN de nivel 1, define una red virtual según los puertos de conexión del conmutador:

[6]http://polaris.lcc.uma.es/-eat/services/rvirtual/rvirtual.html#link 1

VENTAJAS[7]:

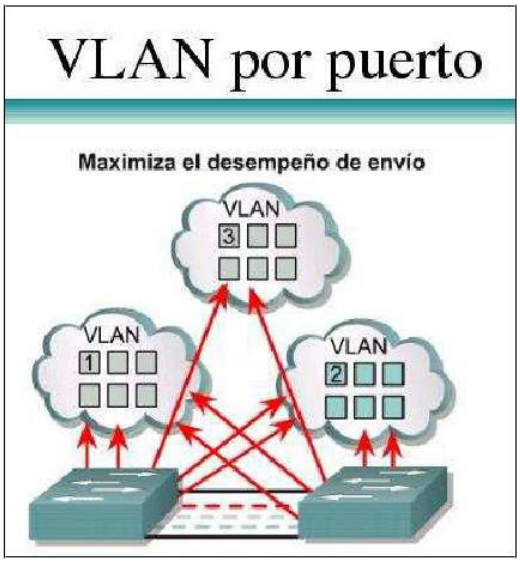
- **Facilidad de movimientos y cambios. -** Un movimiento supone que la estación cambia de ubicación física, pero sigue perteneciendo a la misma VLAN. Requiere reconfiguración del puerto al que se conecta la estación salvo si se utilizan técnicas de asignación dinámica a VLAN. Y LA ESTACIÓN PUEDE precisar reconfiguración (por ejemplo, si se utiliza protocolo IP sin servidor DHCP). La reconfiguración de la estación no será necesaria si la subred (IP, IPX, etc.) a la que pertenece está totalmente contenida en la VLAN. Cualquier operación de añadir, mover o cambiar un usuario se traduce normalmente en la configuración de un puerto y algunas aplicaciones gráficas de gestión de VLANs automatizan totalmente esta reasignación.
- **Microsegmentación y reducción del dominio de broadcast. -** aunque los conmutadores permiten dividir la red en pequeños segmentos, el tráfico broadcast sigue afectando al rendimiento de las estaciones y se precisan routers o VLANs para aislar los dominios de broadcast. La definición de VLANs por puerto implica que el tráfico de broadcast de una VLAN no afecta a las estaciones en el resto de VLANs puesto que es siempre interno a la VLAN en la que se origina.
- **Multiprotocolo.-** la definición de VLANs por puerto es totalmente independiente del protocolo o protocolos utilizados en las estaciones. No existen pues limitaciones para protocolos de uso poco común como VINES, OSI, Etc. o protocolos dinámicos como DHCP.

[7] http://www.ibw.com.ni/-alanb/campus.html

DESVENTAJAS[8]:

- **Administración.-** Los movimientos y cambios implican normalmente una reasignación del puerto del conmutador a la VLAN a la que pertenece el usuario. Aunque las aplicaciones de gestión facilitan esta tarea es recomendable combinar dichas aplicaciones con mecanismos de asignación dinámica de VLAN de forma que se asignen los puertos a la VLAN en función de LA dirección MAC o de otros criterios como la dirección de nivel 3. cisco ha desarrollado un método de asignación dinámica de red VLAN a puerto basándose en las direcciones MAC de las estaciones de red.

Figura 1.4: Vlan Por Puerto



FUENTE: https://www.google.com.pe/search?gs_rn=25&gs_ri=psy-ab&tok=WVJ1zmY-NY5RdRwqK8dhVA&cp=4&gs_id=q&xhr=t&q=nsfnet&bav=on.2,or.r -

[8] http://www.ibw.com.ni/-alanb/campus.html

VLAN DIRECCION MAC.

También denominada VLAN de nivel 2. Define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que las VLAN basado en puerto, ya que la red es independiente de la ubicación de la estación.

VENTAJAS[9]

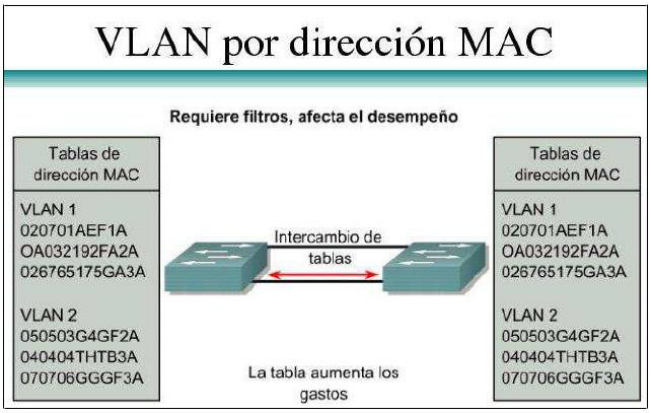
- **Facilidad de movimientos. -** No es necesario en caso de que una terminal de trabajo cambie de lugar de re-configuración del switch.
- **Multiprotocolo.**
- **Se puede tener miembros en múltiples VLANs.**

DESVENTAJAS[10]

- **Problemas de rendimiento y control de Broadcast:** El tráfico de paquetes de tipo Multicast y Broadcast se propagan por todas la VLANs.
- **Complejidad en la administración:** En un principio todos los usuarios se deben configurar de forma manual. Las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

[9] http://www.ibw.com.ni/-alanb/campus.html
[10] http://www.ibw.com.ni/-alanb/campus.html

Figura 1.5: Vlan Por Dirección Mac



VLAN POR FILTROS.

La asignación a las Vlans se basa en información de protocolos de red (por ejemplo dirección IP, o dirección IPX y tipo de encapsulación). La pertenencia a la VLAN se basa en la utilización de unos filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN. Los filtros han de aplicarse por cada trama que entre por uno de sus puertos del conmutador.

VENTAJAS[11]

- **Segmentación por protocolo. -** Es el método apropiado solo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en el tipo de protocolo de nivel 3 y la segmentación física existente sea muy diferente a los patrones de direccionamiento.

[11] http://www.ibw.com.ni/-alanb/campus.html

- **Asignación dinámica. -** tanto la definición de VLANs por dirección MAC COMO por protocolo de nivel 3 ayudan a automatizar la configuración del puerto del conmutador en una VLAN determinada.

DESVENTAJAS[12]

- **Problemas de rendimiento y control de Broadcast:** La utilización de VLANs de nivel 3 requiere complejas búsquedas en tablas de pertenencia que afectan al rendimiento global del conmutador. Los retardos de transmisión pueden aumentar entre un 50% a un 80%
- **No soporta protocolos de nivel 2 ni protocolos dinámicos. -** La estación necesita una dirección de nivel 3 para que el conmutador le asigne una VLAN. Las estaciones que utilicen protocolos de nivel 2 como NetBios y LAT no podrán asignarse a una VLAN. Las estaciones que utilicen protocolos de nivel 2 como NetBios y LAT no podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y la estación no tiene configurada su dirección IP ni su router por defecto el conmutador no puede clasificar la estación dentro de una VLAN. Una premisa esencial en la definición de Vlans es que el rendimiento del conmutador no debe degradarse debido a la existencia de Vlans. Las técnicas de marcado (identificación de paquetes pertenecientes a cada VLAN) utilizadas en la definición de Vlanspor puerto permiten mantener una velocidad de transmisión según el ancho de banda disponible (wirespeed performance – rendimiento de velocidad en el cable) y por ello ha prevalecido dicha solución en la definición del estándar 802.1Q.

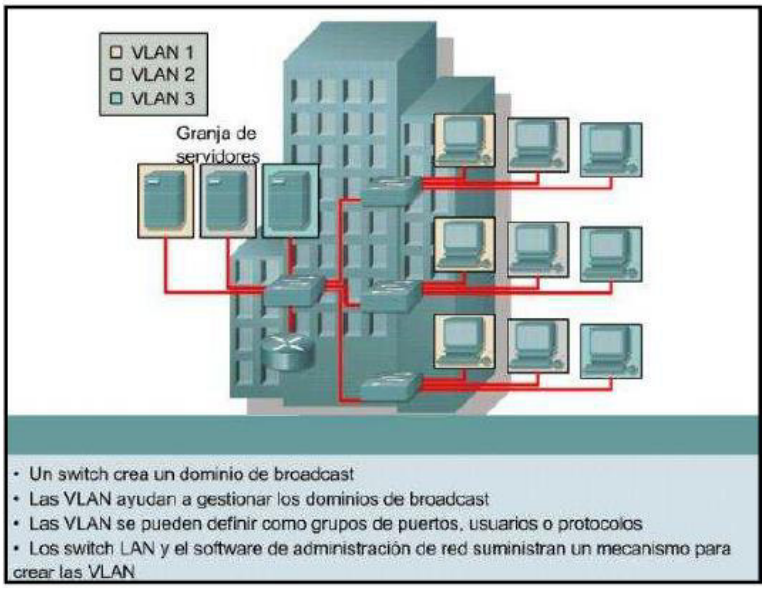
[12] http://www.ibw.com.ni/-alanb/campus.html

estas técnicas permiten además la asignación de un mismo puerto o tarjeta de red a varias Vlans (router o servidores pueden aprovechar esta ventaja evitándose la utilización de tantos interfaces o tarjetas de red como Vlans). ISL (Inter-Switch- Link) para Fast Ethernet / Token Ring y 802.10 para FDDI son dos ejemplos de técnicas de mercado.

DOMINIO DE BROADCAST.

Una VLAN es un dominio de broadcast que se crea en uno o más switches.

Figura 1.6: Dominio de Broadcast en las Vlans

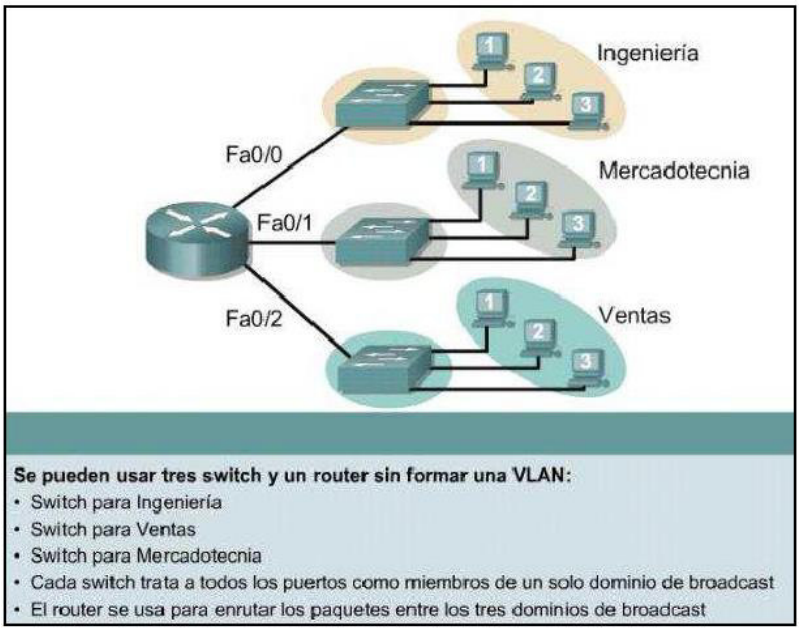


Para poder asimilar de mejor manera lo que significa el dominio de broadcast se utilizará algunos ejemplos.

Ejemplo 1[13]: en la siguiente figura se muestra como los tres dominios de broadcast se usan creando tres switches. El enrutamiento de capa 3 permite que el router mande los paquetes a tres dominios de broadcast diferentes.

[13] http://www.tml.unavarra.es/asignaturas/aro/ccna3-8.ppt

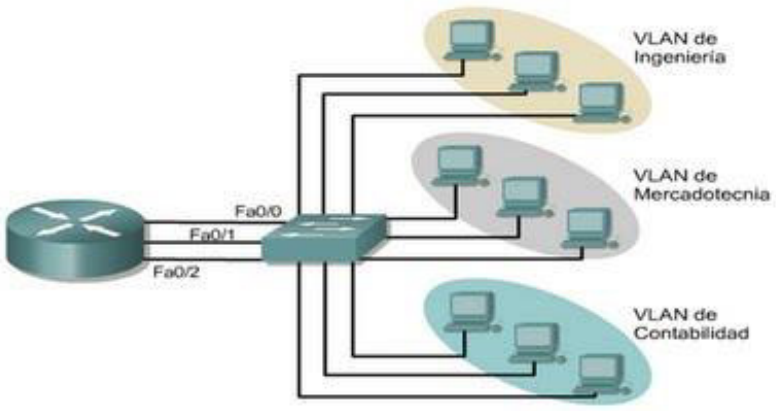
Figura 1.7: Ejemplo de la utilización de un router con la Vlan.



FUENTE:

Ejemplo 2[14]: Tres dominios de broadcast separados

Figura 1.8: Ejemplo de tres dominios de broadcast separados



En esta figura se crea una VLAN con un router y un switch. Existen tres dominios de broadcast separados. El routerenruta el tráfico entre las VLAN mediante

[14]http://www.tml.unavarra.es/asignaturas/aro/ccna3-8.ppt

enrutamiento de capa 3. El switch en la figura envía tramas a las interfaces de los router cuando se presentan ciertas circunstancias.

- Si es una trama de broadcast.
- Si está en la ruta a una de las direcciones MAC del router.

COMPONENTES DE LAS VLANS.

Los componentes físicos de las VLAN son los equipos que soportan los estándares de comunicación de las Vlans, esto incluye switches, puentes, interfaces de red, etc., todos los dispositivos con los que se implante un modelo de red con Vlan.

El componente principal de una Vlan es el estándar de comunicación que utiliza, en el caso particular es el estándar IEEE 802.1Q.

El estándar IEEE 802.1Q define una arquitectura para las LAN con Puentes virtuales, los servicios proporcionados en las VLAN, y los protocolos y algoritmos que participan en la oferta de estos servicios.

SEGURIDAD EN LAS VLANS

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que se tomen, por lo que se debe hablar de niveles de seguridad. La seguridad informática es un

conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos. Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque hardware, software y datos; son datos y la información los sujetos principales de protección de las técnicas de seguridad.

La seguridad informática se dedica principalmente a proteger la confidencialidad se refiere a que la información sólo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos[15].

La seguridad en las VLANS depende de forma primordial de la administración, y de las prestaciones de los equipos que se utilicen para formar las VLANS, cabe mencionar que mientras más segura y con menos accesos en una red la administración de la misma es más compleja.

La seguridad que se tiene en una VLAN específica es muy elevada, puesto que solo los miembros que pertenecen a dicha VLAN podrán compartir recursos, como si fuese una LAN creada sólo para ese grupo determinado.

Es necesario indicar que si no hay una distribución correcta de los usuarios que pertenecen a una VLAN determinada o, si se empiezan a trasladar usuarios de una VLAN general a la VLAN específica segura, subirá el riesgo de inseguridad de los datos a través de dicha VLAN.

[15] http://www.solocursosgratis.com/curso_gratis_seguridad_informatica_-_conceptos_basicos-slccurso1029234.htm

BENEFICIOS DE LA IMPLEMENTACION DE LAS VLANS

Para poder comprender de mejor manera los beneficios que tienen las redes virtuales (VLANS) se debe tener claro cómo funciona una red basada en enrutadores. Los enrutadores utilizan la capa tres del modelo OSI para mover tráfico en la red local LAN a otra red (Alcocer, 2000).

Cada capa contiene campos en los cuales se identifica el dominio de broadcast en el cual el destino puede ser encontrado. Estas direcciones están asignadas por un administrador de red, y son generalmente registradas dentro de los archivos de configuración de las estaciones de red.

En una red basada en concentradores y enrutadores la dirección de red identifica un segmento de la misma[16].

Teniendo claro esto, cuando se cambia a una red virtual se obtiene los siguientes beneficios[17].

- Las redes virtuales hacen que se reduzca el costo de manejo de usuarios que se mueven y cambian, este beneficio se obtiene principalmente en las VLANs que han sido implementadas en el nivel 3 con direcciones IP, debido a que la estación que cambia de sitio conserva su dirección IP; cosa que no sucede en las redes LAN pues si el dispositivo o estación de red es movido de un concentrador a otro, la dirección de red ya no será válida y el administrador de la red deberá corregir los archivos de configuración.

[16] http://lauca.usach.cl/-lsanchez/Vlan
[17] http://lauca.usach.cl/-lsanchez/Vlan

- Con las redes virtuales se pueden se pueden establecer Grupos de Trabajo Virtuales, esto es, miembros de un mismo departamento que están conectados en la misma LAN, es decir, físicamente contiguos pueden estar en diferentes VLANs. Así, si se cambia la estación del sitio pero en el mismo departamento no se tiene que reconfigurar la máquina; si el equipo cambia de VLAN solo hay que cambiar su número de red virtual y no su lugar físico.
- Otra ventaja es que se puede establecer estos grupos de trabajo con el criterio 80/20 el cual consiste en el 80% del tráfico de información es en la misma VLAN o grupo de trabajo y solamente el 20% restante es entre VLANs y por lo tanto no se requieren muchos enrutadores.
- Acceso a recursos: un recurso y servidor puede estar en dos redes virtuales diferentes al mismo tiempo, es decir las VLANs permiten superposición lo que reduce considerablemente el tráfico entre redes virtuales diferentes.
- Uno de los beneficios principales es la reducción de enrutadores cuando se tiene una LAN los dominios de broadcast, son determinados por los enrutadores, en cambio, en una VLAN un switch sabe cuáles puertos pertenecen al dominio de broadcast y por lo tanto solamente envía información a esos puertos, sin necesidad de un enrutador.
- Las VLANs pueden llegar a ser muy seguras cuando se implementan en conjunto con switches con puerto privado. Se pueden implementar un firewall en cada VLAN fácilmente, éste es un servidor encargado de la seguridad, estableciendo permisos de entrada a cada red virtual.

- Dependiendo de la inteligencia de los switches se puede hacer filtrado e intercambio de decisiones respecto a los paquetes que pertenecen al tráfico, basados en medidas adoptadas por los administradores de la red. Esto se puede realizar a través de métodos como el filtrado de paquetes y de la identificación de paquetes (encapsulado).
- Control y conservación del ancho de banda, las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un dominio determinado o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.
- Protección de la inversión, las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la res o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costos adicionales.
- Otro punto a destacar es que la tecnología ATM prevé, como parte importante de sus protocolos, grandes facilidades para las redes virtuales, lo que equivaldrá sin duda a grandes ventajas frente a la competencia para aquellos equipos que actualmente ya soportan sistemas VLAN.
- Se puede controlar el tráfico de broadcast de 2 maneras: limitando el número de puertos en el switch o limitando el número de personas que usan los puertos.

Estas diferencias entre los dos tipos de redes hacen de las redes virtuales una solución más económica desde el punto de vista de desempeño y rapidez del flujo de información. Como los enrutadores no se usan para crear y separar cada dominio de broadcast, la disposición entre sus funciones principales es:

- Proveer conectividad entre las diferentes VLANs.
- Ser un filtro de broadcast para los enlaces WAN.

LISTAS DE CONTROL DE ACCESO – ACL.

Las listas de Control de Acceso (ACL / Access Control List) incluyen una de descripción de los usuarios y grupo de usuarios con diferentes permisos sobre los archivos y carpetas de un volumen NTFS (New Technology File System).

Aparecer en la lista ACL significa tener derecho de acceso sobre el archivo o carpeta. El tipo de permiso definido en la entrada de un usuario o grupo de usuarios específica el nivel de privilegio sobre el objeto (lectura, escritura, etc.)

Cada vez que un usuario accede a un archivo o carpeta se verifica si el usuario o el grupo de usuarios al que pertenece tienen al menos una entrada en la lista ACL del objeto. De no ser así el sistema le niega el derecho sobre el objeto; en cambio, si posee uno o más entradas, el usuario podrá acceder al objeto con los privilegios especificados por los permisos asociados a las entradas.

DEFINICION DE CALIDAD DE SERVICIO (QoS)

QoS hace referencia a la capacidad de una red para proporcionar diferentes niveles de servicio al tráfico de red en diversas tecnologías. Los objetos principales del QoS es el ancho de banda dedicado. Controlar el jitter y la latencia (requerido por algunos servicios en tiempo real y el tráfico interactivo) y la pérdida de características mejoradas.

Las técnicas de trabajo en una congestión de una red, se utilizan para administrar y priorizar el tráfico en una LAN donde las aplicaciones solicitan más ancho de

banda y que la red no es capaz de proporcionar. Al dar prioridad a ciertas clases de tráfico, estas técnicas permiten a las empresas retrasar las aplicaciones sensibles para que funcionen correctamente en una red congestionada.

QoS se puede dividir en tres niveles diferentes. Estos modelos de servicio se pueden describir en un conjunto de capacidades QoS de extremo a extremo.

QoS extremo a extremo, es la habilidad de la red proporcionar un nivel específico de servicio de tráfico de un extremo a otro de la red. Los tres niveles de servicio son: El de mejor esfuerzo de servicio, servicio integrado y servicio diferenciado.

Mejor esfuerzo de servicio, como su nombre lo indica, es cuando la red hará todo lo posible para entregar el paquete del servicio a su destino. Con el mejor esfuerzo no hay garantías de que el paquete alcance su rumbo.

Modelo de servicio integrado, permite a las aplicaciones tener un servicio garantizado mediante la negociación de parámetros de red de extremo a extremo. Las aplicaciones pueden solicitar un nivel de servicio necesario para que funcionen correctamente y confiar en el mecanismo de calidad de servicio para reservar los recursos de red necesarios antes de que se inicie la transmisión de los paquetes de la aplicación. Es importante señalar que la aplicación no envía algún tipo de tráfico hasta que reciba una señal de la red la cual le indica que la red puede manejar la carga y entregar a su destino un QoS.

Modelo de servicios diferenciados. El cual incluye un conjunto de herramientas de clasificación y gestión de colas para la prestación de algunos protocolos o aplicaciones con una cierta prioridad sobre el tráfico de la red. Los servicios

diferenciados se basan en los routers de extremos para realizar la clasificación de los diferentes tipos de paquetes que pasan por una red.

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y video vigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de manera distinta para cada tipo de servicio (voz, datos y video) del tráfico de la red. Al utilizar la calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

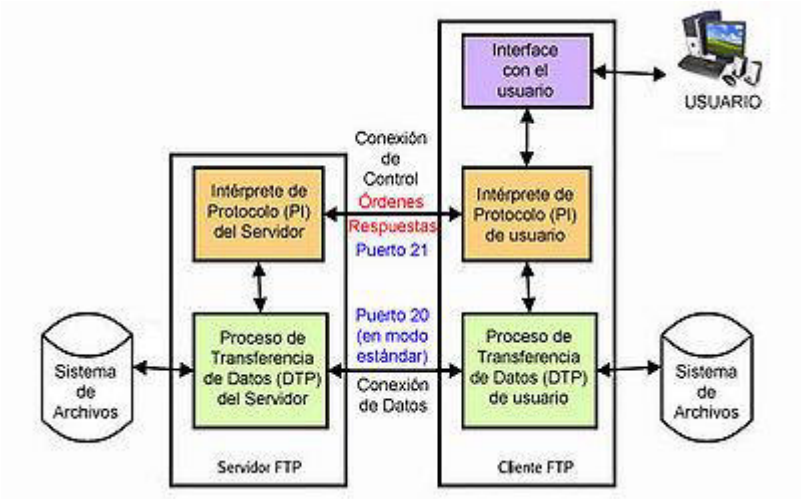
FTP (File Transfer protocol)

FTP (Protocolo de Transferencia de Archivos), es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmissión Control Protocol), basado en la arquitectura cliente – servidor (Tanenbaum, 2003). Desde un equipo cliente se puede conectar a un servidor para descargar, enviar archivos independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensando para ofrecer la máxima seguridad ya que todo el intercambio de información desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico,

acceder al servidor, o apropiarse de los archivos transferidos. Para solucionar este problema son de gran utilidad aplicaciones como Scp y Sftp, incluidas en el paquete SSh, que permiten transferir archivos pero cifrando todo el tráfico.

Figura 1.9: Diagrama de un servidor FTP



FUENTE: http://es.wikypedia.orgwiki/File_Transfer_Protocol

a) Servidor FTP.

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes LAN, MAN, etc.) Su función es permitir el intercambio de datos entre diferentes servidores/ ordenadores (Barceló, 2004).

Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus

archivos correspondientes; o como servidor de backup (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol).

b) Cliente FTP.

Cuando un navegador no está equipado con la función FTP, o si se quiere cargar archivos en un ordenador remoto, se necesita utilizar un programa cliente FTP es un programa que se instala en el ordenador del usuario y que se emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos ya para descargarlos o para subirlos.

Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el ordenador en que reside (servidor en el caso de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra.

c) Ventajas de los FTP.

Los programas FTP permiten reanudar las descargas interrumpidas por cortes de conexión o cualquier otra circunstancia en el mismo punto donde se quedaron.

Son tan fáciles de usar con el Explorador de Windows no hay que utilizar complicados comandos ni teclear orden alguna. Para descargar un archivo

basta con arrastrarlo con el mouse desde una ventana (el servidor remoto) a otra (el disco duro).

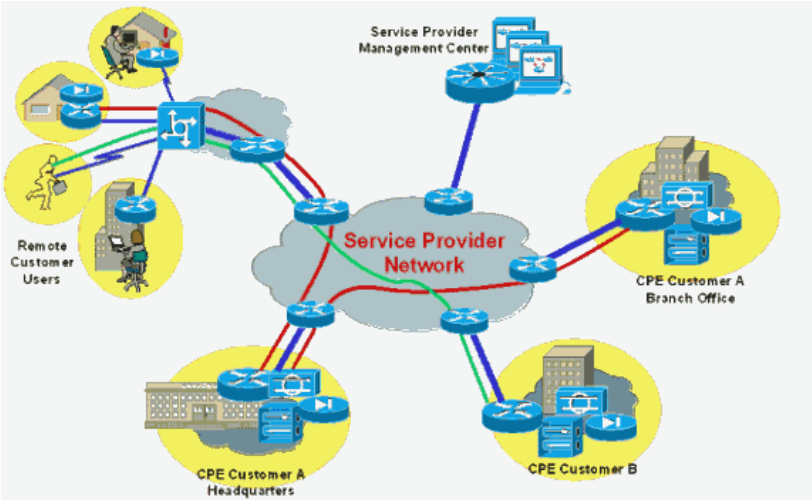
Permiten hacer descargas masivas y automatizadas en segundo plano, mientras se realizan otras tareas con el computador: así el usuario puede despreocuparse de la descarga hasta que finaliza.

También facilitan la transferencia de archivos de un servidor remoto a otro. En la mayoría de los casos, servidor remoto a otro. En mayoría de los casos, estas transferencias son mucho más rápidas que cuando se realizan a través de la conexión personal.

REDES PRIVADAS VIRTUALES (Vpn)

Muchas compañías tienen oficinas e instalaciones esparcidas en muchas ciudades, algunas veces en múltiples países. En el pasado, antes de que existieran las redes de datos públicas, era común qué algunas compañías alquilaran líneas a las compañías telefónicas entre todas o entre sólo algunas ubicaciones. Algunas compañías aún hacen esto. Una red constituida por computadoras de compañías y líneas telefónicas alquiladas se conoce como red privada.

Figura 110: Red Privada Virtual



Fuente:

Las redes privadas funcionan bien y son muy seguras. Si las únicas líneas disponibles son las alquiladas, el tráfico no puede fugarse de las ubicaciones de la compañía y los intrusos tienen que intervenir físicamente las líneas para infiltrarse, lo cual no es fácil de hacer. El problema con las redes privadas es que alquilar una sola línea T1 cuesta miles de dólares mensuales y las líneas T3son muchas veces más costosas. Cuando aparecieron las redes de datos públicas y, más tarde, Internet, muchas compañías quisieron trasladar su tráfico de datos (y, posiblemente, de voz) a la red pública, aunque sin renunciar a la seguridad de la red privada.

Esta demanda pronto llevó a la invención de las **VPNs** (**redes privadas virtuales**)**,** que son redes superpuestas sobre redes públicas, pero con muchas propiedades de las redes privadas. Se llaman “virtuales” porque son sólo una ilusión, al igual que los circuitos virtuales no son circuitos reales ni la memoria virtual es memoria real.

Aunque las VPNs pueden implementarse encima de ATM (o de FrameRelay), un método cada vez más popular es construir VPNs directamente sobre Internet. Un diseño común es equipar cada oficina con un *firewall* y crear túneles a través de Internet entre todos los pares de oficinas. Si IPsec se utilizara para el proceso de entunelamiento, entonces sería posible agregar todo el tráfico entre cualquiera de los dos pares de oficinas en una sola SA encriptada y autenticada, con lo que se proporcionaría control de integridad, confidencialidad e incluso inmunidad considerable al análisis de tráfico.

Cuando se inicia el sistema, cada par de *firewalls* tiene que negociar los parámetros de su SA, incluyendo los servicios, modos, algoritmos y claves. Muchos *firewalls* tienen capacidades VPN integradas, aunque algunos enrutadores ordinarios también pueden hacer esto. Pero debido a que los *firewalls* están principalmente en el negocio de la seguridad, es natural que los túneles empiecen y terminen en los *firewalls*, estableciendo una clara separación entre la compañía e Internet. Por lo tanto, los *firewalls*, las VPNs e IPsec con ESP en modo de túnel son una combinación natural y se utilizan ampliamente en la práctica.

Una vez que se han establecido las SAs, el tráfico puede comenzar a fluir. Para un enrutador en Internet, un paquete que viaja a través de un túnel VPN es sólo un paquete ordinario. Lo único extraño es la presencia del encabezado IPsec después del encabezado IP, pero debido a que estos encabezados adicionales no tienen efecto en el proceso de reenvío, los enrutadores no se preocupan por ellos.

Una ventaja principal de organizar de esta forma una VPN es que es completamente transparente para todo el software de usuario. Los *firewalls* configuran y manejan las SAs. La única persona que está consciente de esta configuración es el administrador del sistema, quien tiene que configurar y manejar los *firewalls*. Para todos los demás, es como tener nuevamente una red privada mediante una línea alquilada.

HERRAMIENTAS DE SIMULACION – REDES.

Simulación.

La simulación es la imitación del funcionamiento de un sistema real durante un intervalo de tiempo. Esta simulación puede realizarse ya sea de forma manual o en forma computacional.

Actualmente las herramientas de simulación son de gran utilidad debido a que se puede prever el comportamiento de un sistema antes de implementarlo, se pueden encontrar comportamientos del sistema que no se detectan fácilmente por la complejidad del estudio y una razón muy importante en cualquier empresa es el ahorro del dinero porque ayuda al diseño y perfeccionamiento del sistema a construir.

Existen muchos software de simulación los que no necesitan que se realce un análisis del sistema para desarrollar el sistema, sino que solo se requieren datos de entrada para su uso, los cuales también brindan facilidades de uso y análisis de los resultados entregados.

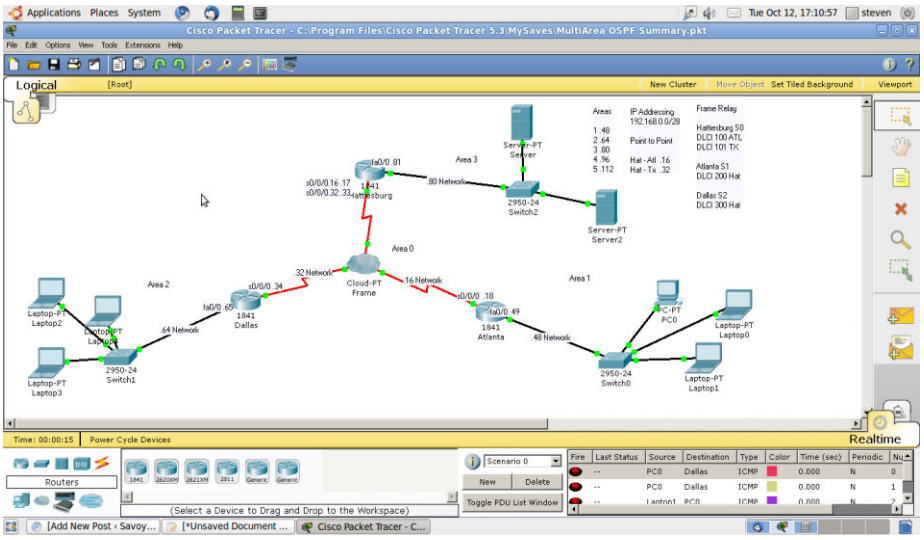
CISCO PACKET TRACER

Es un software para crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Se apoya en mejorar los protocolos de red. Hoy en día es la herramienta de simulación más utilizada, conforme los productos de la Familia Cisco van ganando terreno en el mercado de equipos orientados al soporte de la plataforma de Red. Soporta los siguientes protocolos:

- HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP Y DNS.
- TCP/UDP, IPv4, IPv6, ICMPv4 E ICMPv6.
- RIP, EIGRP, OSPF Multitarea enrutamiento estático y redistribución de rutas.
- Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP, ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP, Polly Mkt.

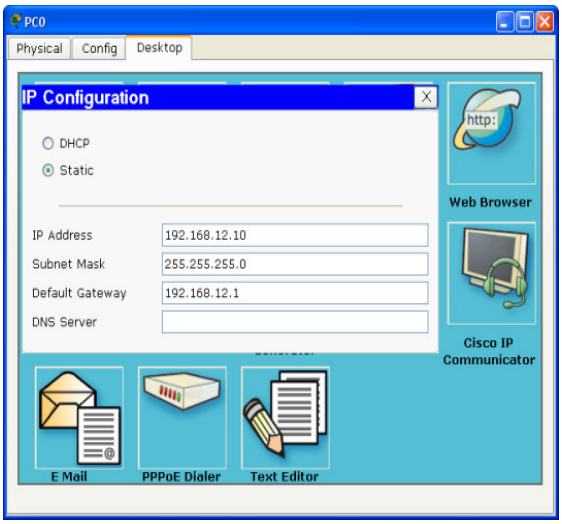
Figura 1.11: Cisco Packet Tracer

Figura 1.12: Diseñando una topología de red en Cisco Packet Tracer



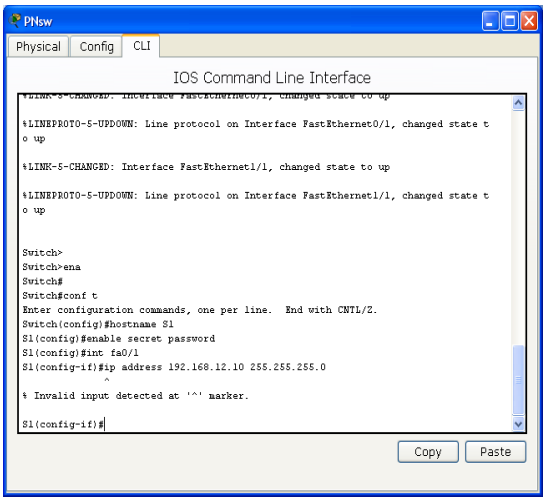
FUENTE: Elaboración propia.

Figura 1.13: Configurando la PC0



FUENTE: Elaboración propia.

Figura 1.14:Configurando por modo consola



FUENTE: Elaboración propia

GNS3

GNS3 es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
- Dynagen, un front-end basado en texto para Dynamips
- Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco o las personas que quieren pasar sus CCNA, CCNP, CCIE, DAC o certificaciones (Delgado, 2009).

Figura 1.15: Simulador GNS3

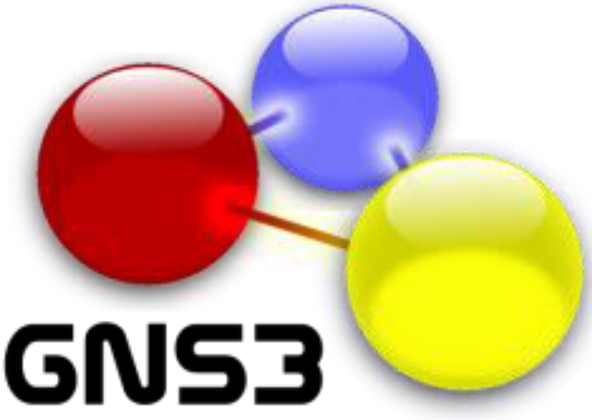
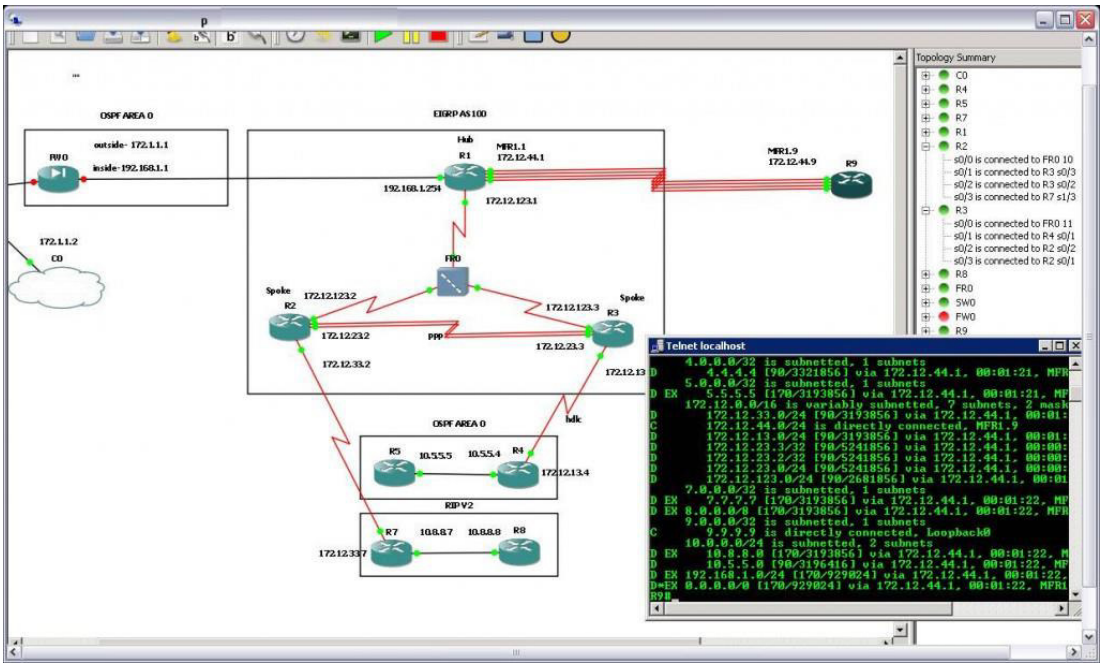


Figura 1.16: Simulando en GNS3



FUENTE:

FORMAS DE IMPLEMENTACION.

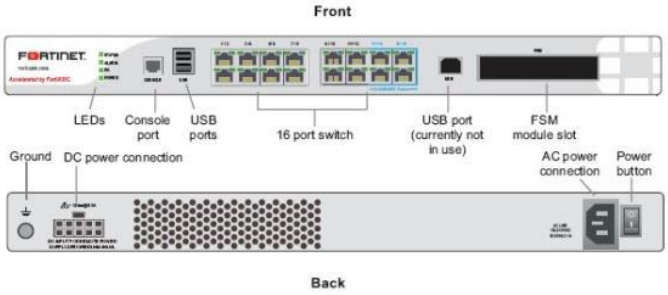
Figura 1.17 Topología básica de una Vlan

FUENTE: Elaboración propia

USANDO EL FIREWALL 200b poe

Para crear Vlans con el firewall **Fortinet 200b poe** se procede de la siguiente manera:

Figura 1.18 Firewall FORTINET 200b POE



FUENTE: http://www.avfirewalls.com.au/FortiGate-200B.asp

ADICIONANDO SUBINTERFACES VLAN.

A. EN MODO NAT / RUTA

1. Vaya a System >Network> Interfaces.
2. Seleccione “Create new” para añadir una subinterfaz VLAN.
3. Introduzca un nombre para identificar la subinterfaz VLAN.
4. Seleccione la interfaz física que recibe los paquetes destinados a esta VLAN subinterfaz VLAN.
5. Introduzca el ID de VLAN que coincida con el ID de VLAN de los paquetes que se reciben por esta subinterfaz VLAN.
6. Seleccione el dominio virtual al que agregar esta subinterfaz VLAN
7. Seleccione el nombre de una zona si desea que esta subinterfaz VLAN pertenezca a una zona.
8. Configure los ajustesde la subinterfaz VLAN como si se tratara de cualquier interfaz Fortigate.
9. Seleccione “OK” para guardar los cambios. La unidad de Fortiigate agrega la nueva subinterfaz VLAN de la interfaz que usted selecciono en el paso 4.☒

Para agregar las políticas del Firewall a las interfaces VLAN.

Una que vez que se agregado subinterfaces VLAN que permita una política de Firewall para las conexiones entre subinterfaces VLAN o de una interfaz VLAN de una interfaz física.

1. Vaya a Firewall>Address.
2. Seleccione “CreateNew” para añadir direcciones de servidor de seguridad que coinciden con las direcciones IP origen y destino de los paquetes de la VLAN.
3. Vaya a Firewall >Polícy.
4. Añadir las políticas de Firewall según sea necesario.

B. EN MODO TRANSPARENTE.

1. Vaya a System >Network> Interface.
2. Seleccione “Create New” para agregar una subinterfaz VLAN.
3. Introduzca un nombrepara identificar la subinterfaz VLAN.
4. Seleccione la interfaz física que recibe los paquetes destinados a esta VLAN subinterfaz VLAN.
5. Introduzca el ID de la VLAN que coincida con el ID de VLAN de los paquetes que se reciben por esta subinterfaz VLAN.
6. Seleccione el dominio virtual que agregar a esta subinterfaz VLAN.
7. Active o desactive el uso de un servicio de DNS dinámico (DDNS). Si la unidad de Fortigate utiliza una dirección IP dinámica, se puede arreglar con un proveedor de servicios DDNS para usar un nombre de dominio.
8. Configurar el acceso administrativo, MTU y la configuración del registro como lo haría para cualquier interfaz Fortigate.

9. Seleccione “OK” para guardar los cambios. La unidad Fortigate agrega la nueva subinterfaz a la interfaz que usted seleccionó.
10. Seleccione “Bring up” para iniciar la subinterfaz VLAN.

Para agregar las políticas deFirewall para subinterfaces VLAN.

Una vez que haya agregado subinterfaces VLAN que permiten una política de Firewall para conexiones entre las subinterfaces VLAN o de una subinterfaz VLAN a una interfaz física.

1. Vaya a Firewall >Address.
2. Seleccione “CreateNew” para añadir direcciones de servidores de seguridad que coincidan con la IP de origen y destino de los paquetes de la VLAN.
3. Vaya a Firewall >Polícy.
4. Añadir políticas según sea necesario.

USANDO EL SWITCHhp V1905.

Figura 1.19 Switch hp v1905

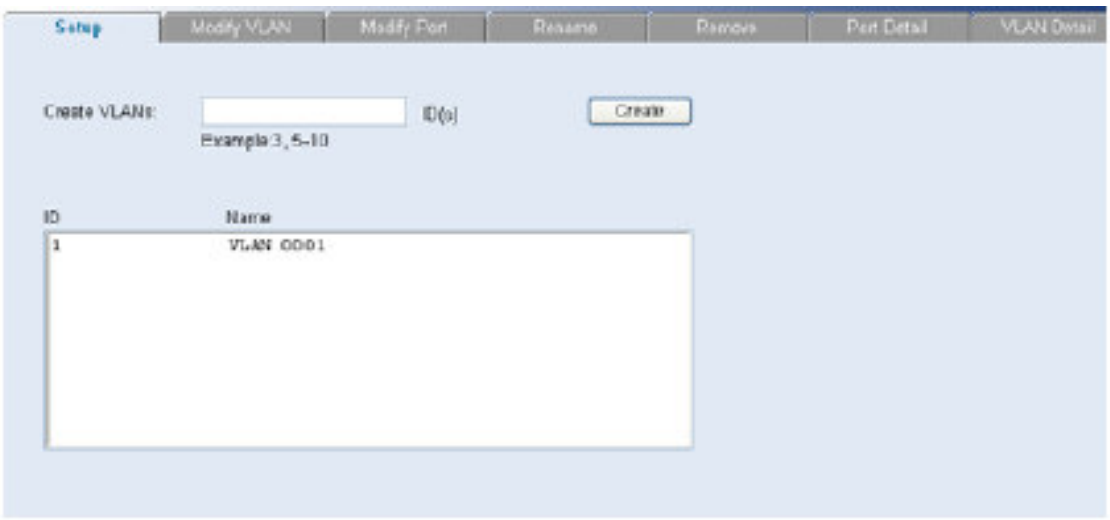
FUENTE: http://www.shopping.com/Hewlett-Packard-HP-V1905-24-Switch-Switch-Managed-24-ports-Ethernet-Fast-Ethernet-10Base-T-100Base-TX/info

CREAR O CAMBIAR EL NOMBRE DE UNA VLAN.

La página de configuración VLAN,permite al administrador de red para **crear** o para **cambiar** el nombre de la VLAN.

- Click**Device** → VLAN → **Setup.** La página de configurar VLAN se abre.

Figura 1.20 Interfaz de configuración - Setup



La página de configuración de VLAN contiene los siguientes campos:

Tabla 2.1 Configuración de Vlan

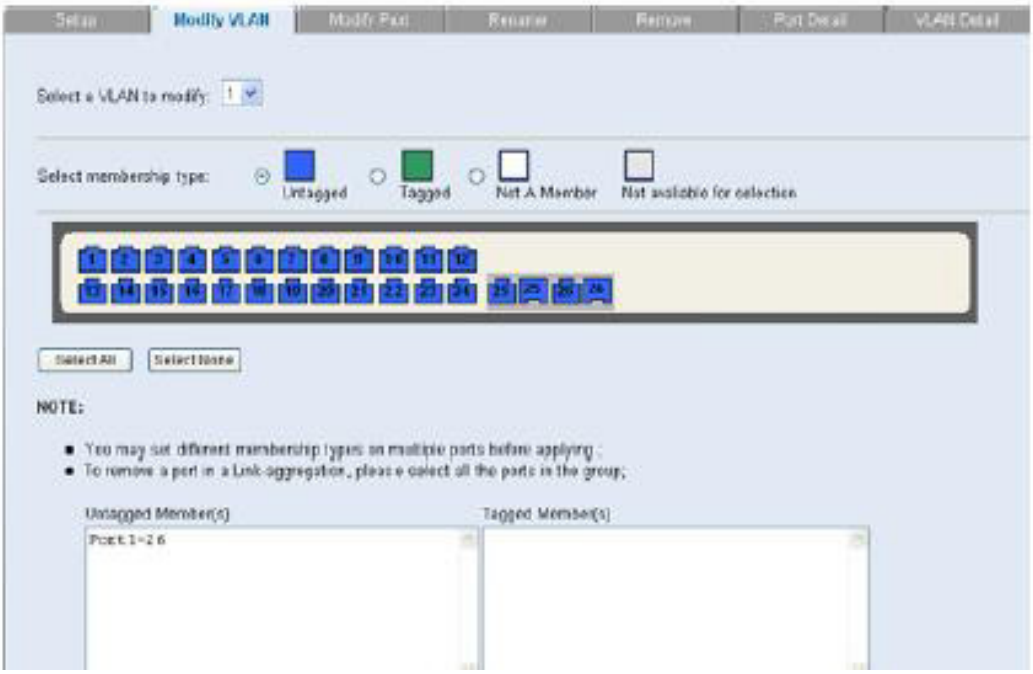
ITEM	DESCRIPCION
CreateVLANs	Ingrese el ID de las VLANs creadas.
Create	Crea el ID de la VLAN.
ID	Muestra el ID de la VLAN.
Name	Muestra el nombre de la VLAN definido por el usuario.

MODIFICACION DE VLAN.

La página de modificación de VLAN permite al administrador de red cambiar la afiliación de VLAN.

- Click → **Device** → **VLAN** → **Modify VLAN**. La página de modificación de VLAN se abre.

Figura 1.21 Interfaz de configuración – Modificar Vlan



La página de modificación de VLAN contiene los siguientes campos:

Tabla 2.2 Modificación de Vlan

ITEM	DESCRIPCION
Select a VLAN to modify.	Seleccione una VLAN para modificar su configuración.
Selectmembershiptype	Seleccione el tipo de membrecía para cada puerto en la VLAN. los posibles valores de campo son:

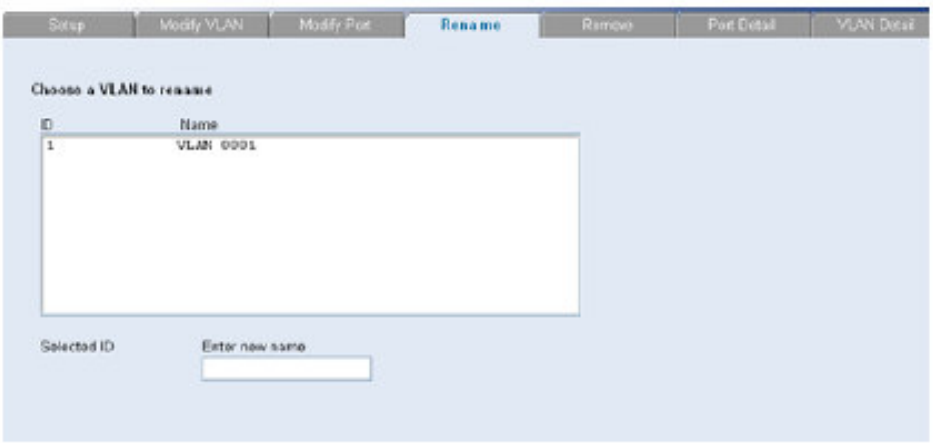
	• **Untagged:** significa que la interfaz es un miembro de la membrecía sin etiquetar. • **Tagged:** indica que la interfaz es un miembro etiquetado de VLAN. • **No a Member:** indica que la interfaz no es miembro de la VLAN. • **No availableforselection:** Indica que la interfaz no está disponible para la selección.
Taggedmembership.	Indica que el puerto es un miembro sin etiquetar de la VLAN.
Untaggedmembership.	Indica que el puerto es un miembro etiquetado de la VLAN.

CAMBIAR EL NOMBRE A LA VLAN.

La página renombrar VLAN, permite al administrador de la red seleccionar una VLAN de la lista para cambiar el nombre.

- Click**Device** → **VLAN** → **Rename.** La página de renombrar VLAN se abre.

Figura 1.22 Interfaz de configuración – Cambiar Nombre



ELIMINAR VLAN.

La pestaña Remove VLAN permite al administrador de la red eliminar una VLAN.

- Click**Device** → **VALN** → **Remove.** La página de eliminar VLAN se abre.

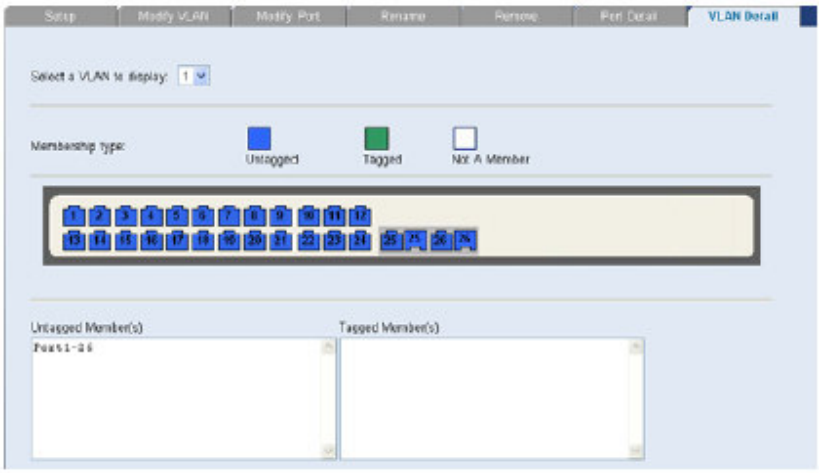
Figura 1.23 Interfaz de configuración – Eliminar Vlan

VIENDO DETALLES DE LA VLAN.

La página Detalle de VLAN, proporciona información y parámetros globales sobre las VLANs configuradas en el sistema.

Click **Device** → **VLAN** → **VALN Detail.** La página detalles de VLAN se abre.

Figura 1.24 Interfaz de configuración – Ver detalles

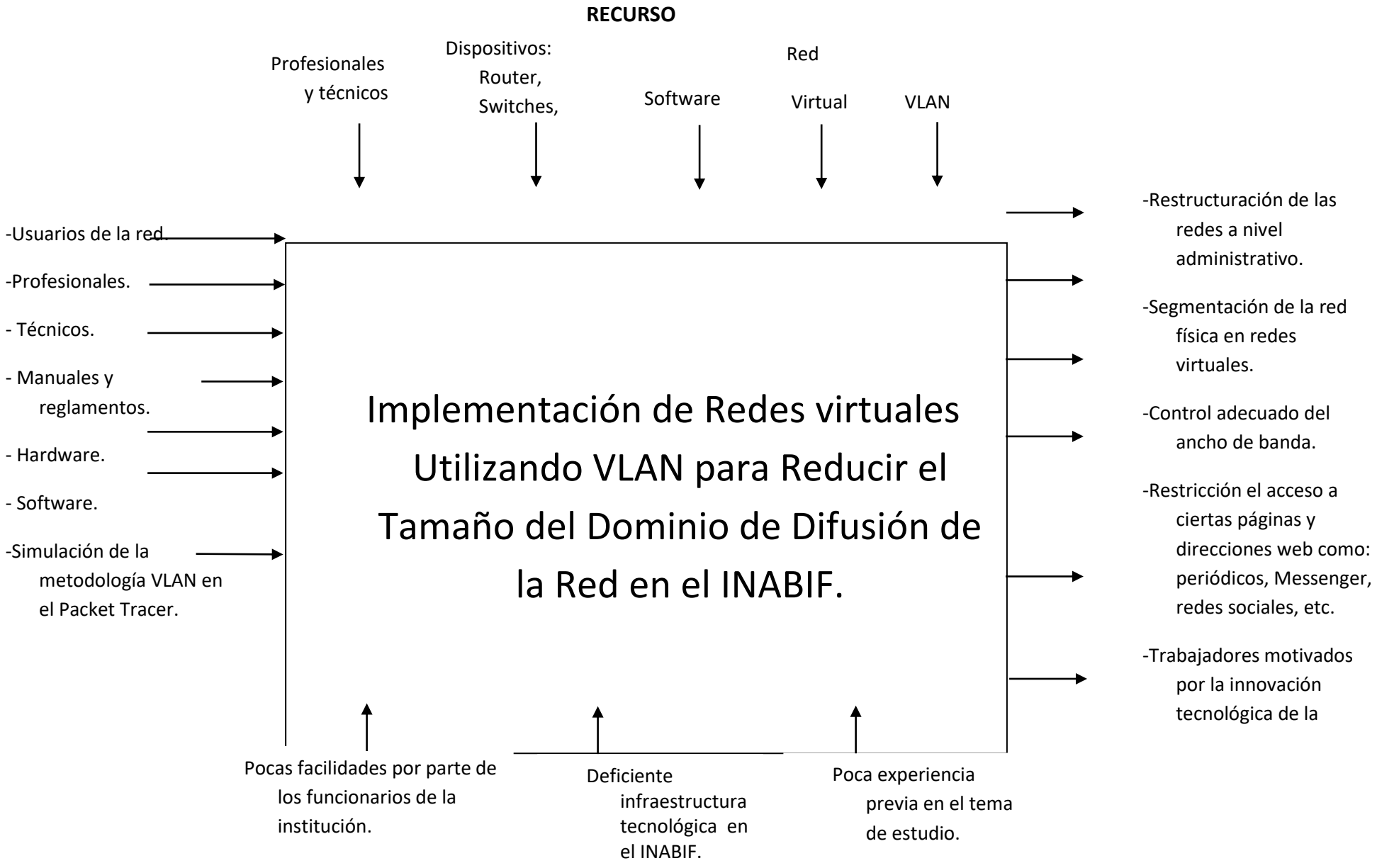


CUADRO COMPARATIVO DE LOS TIPOS DE VLANS.

Tabla 2.3 Tipos de Vlan

VLANs	RED DE TIPO	CARACTERISTICAS	VENTAJAS	DESVENTAJAS
POR PUERTO	Virtual	Cada puerto del conmutador puede asociarse a una VLAN.	-Facilidad de movimientos y cambios. -Microsegmentación. -Multiprotocolo.	-Administración.
POR DIRECCION MAC	Virtual	La relación de pertenencia a VLAN se basa en la dirección MAC.	-Facilidad de movimiento. -Multiprotocolo.	-Problemas de rendimiento y control de brodcast. -Complejidad en la administración.
POR FILTROS	Virtual	La asignación a las VLANS se basa en información de protocolos de red. La pertenencia a la VLAN se basa en la utilización de unos filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN.	-Segmentación por protocolo. -Asignación dinámica.	-Problemas de rendimiento y control de brodcast. -No soporta protocolos de nivel 2 ni protocolos dinámicos.

MODELO GENERAL DE LA SOLUCIÓN.



2.3 MARCO CONCEPTUAL

ACL (Access Control List), es una lista de los servicios disponibles, cada uno con una lista de los host que permitieron usar el servicio.

Ancho de Banda, se refiere a la capacidad de transmisión de un canal. Indica la cantidad de información por unidad de tiempo que puede enviarse a través de una línea de transmisión, medida frecuentemente en bits por segundo (bps).

ARP (Address Resolution Protocol), protocolo de resolución de dirección. Protocolo usado por una computadora para correlacionar una dirección IP con una dirección de hardware. Las computadoras que llaman el ARP difunden una solicitud a la que responde la computadora objetivo.

ATM (Asynchronouse Transfer Mode), modo de transferencia síncrono. Tecnología de transmisión de datos en forma de paquetes. La información se divide en pequeñas células que se transmiten individualmente y se procesan de manera asíncrona.

Backbone, estructura de transmisión de datos de una red o conjunto de ellas en Internet. Literalmente: “esqueleto”

Backups, es un computador diseñado para copiar datos con el propósito de tener una copia de seguridad de la fuente original en caso de daños en la fuente original.

Broadcast, (o en castellano “difusiones”), se producen cuando una fuente envía datos a todos los dispositivos de una red.

Carrier, es un operador de telefonía que proporciona conexión a Internet a alto nivel.

CTI (Computer, Telephon y Integration), Integración de teléfono y computadora.

DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS, pero a través de un servidor DNS.

FIREWALL Mecanismode seguridad de internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados.

FTP,es uno de los diversos protocolos de la red internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Archivos) y es el ideal para transferir datos por la red.

GUI (Graphical User Interface), Interface Gráfica de Usuario.

Host, ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como correo electrónico, Telnet y FTP.

Hosting, servicio de alojamiento de las páginas web que gestionan empresas especializadas. Las empresas que se dedican a este servicio son como los hoteleros de la red: ofrecen espacios para que otras compañías almacenen cualquier información que quieren que sea accesible por una red, desde sus páginas web hasta la información de su red interna o intranet.

HTTP (HyperText Transmission Protocol), protocolo para transferir archivos o documentos hipertexto a través de la red. Se basa en una arquitectura cliente / servidor.

ICMP (Internet Control Message Protocol), es un control usado en el nivel de red. Este protocolo se usa principalmente por los routers de internet, para informar de sucesos inesperados, errores, etc. también se usa para hacer pruebas sobre la red (local o internet), por ejemplo, enviando un comando de petición de eco (ping) a un ordenador, y esperar que responda.

IEEE, corresponde a las siglas del Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos, una asociación estadounidense dedicada a la estandarización. Es una asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos, ingenieros en informática.

IP (Internet Protocol), el producto encargado del direccionamiento (identificación del origen y destino).

IPv4, es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del producto que se implementó extensamente, y forma la base de internet.

ISO (International Organization for Standarization), Organización Internacional responsable de una amplia gama de estándares, incluyendo aquellos relevantes para las redes. ISO es la responsable del modelo de referencia OSI, el modelo más popular.

ISP (Proveedor de Servicios de Internet), empresa u organización que brinda el servicio de conexión a internet.

MAC, en redes de computadoras Media Access Control address cuyo acrónimo es MAC es un identificador físico – un número, único en el mundo, de 48 bits almacenado en fabrica dentro de una tarjeta de red o una interface usada para asignar globalmente direcciones únicas en algunos modelos OSI (Capa 2) y en la capa física del conjunto de protocolos de Internet.

Multicast, es un mensaje que se envía simultáneamente a un grupo de nodos específicos en una red.

Multicasting, es la forma de transferencia de datos en donde es posible enviar información de un solo emisor a muchos puntos de diferentes (receptores) simultáneamente.

Networking, trabajar en red, trabajar en colaboración a través de una red. Término utilizado para referirse a las redes de telecomunicaciones en general.

OSI, modelo para la interconexión de sistemas abiertos (Open Systems Interconnection). Es un modelo teórico de conexión de sistemas, estructurado en 7 capas (física, enlace, red, transporte, sesión, presentación y aplicación).

Ping (Packet Internet Groper), es una utilidad que comprueba el estado de la conexión con uno o varios hosts remotos. El comando Ping utiliza los paquetes de solicitud de eco (protocolo ICMP) y de respuesta de eco para determinar si un sistema IP específico es accesible en una red.

PoE(Power over Ethernet), es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red Ethernet.

QoS (Quality of Service), Calidad de Servicio. Son las tecnologías que permiten aplicar un tratamiento específico a un determinado tipo de tráfico. Ejemplos de mecanismos de QoS son la priorización de tráfico y la garantía de un ancho de banda mínimo. La aplicación de QoS es un requisito básico para poder implantar servicios interactivos (por ejemplovoip).

RAS (Registration, Admision and Status), Registro, Admision y Estatus. Protocolo de comunicaciones que permite a una estación H.323 a través del gatekeeper.

ROUTER Conocido también como enrutador o encaminador de paquetes de un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

SERVIDOR En informática, un **servidor** es un nodo que forma parte de una red, provee servicios a otros nodos denominados clientes.

También se suele denominar con la palabra servidor a:

- Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios

de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

- Una computadora en la que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes, tanto si se trata de un ordenador central (*mainframe*), un miniordenador, una computador personal, una PDA o un sistema embebido; sin embargo, hay computadoras destinadas únicamente a proveer los servicios de estos programas: estos son los servidores por antonomasia.
- Un servidor no es necesariamente una máquina de última generación de grandes proporciones, no es necesariamente un superordenador; un servidor puede ser desde una computadora vieja, hasta una máquina sumamente potente (ej.: servidores web, bases de datos grandes, etc. Procesadores especiales y hasta varios terabytes de memoria). Todo esto depende del uso que se le dé al servidor. Si usted lo desea, puede convertir al equipo desde el cual usted está leyendo esto en un servidor instalando un programa que trabaje por la red y a la que los usuarios de su red ingresen a través de un programa de servidor web como Apache.
- Por lo cual podemos llegar a la conclusión de que un servidor también puede ser un proceso que entrega información o sirve a otro proceso. El modelo Cliente-Servidor no necesariamente implica tener dos ordenadores, ya que un proceso cliente puede solicitar algo como una impresión a un proceso servidor en un mismo ordenador.

STP Par trenzado blindado. Medio de transmisión que consta de dos pares de cable de amplio uso en una gran variedad de implementaciones de red. El cableado STP tiene una capa aislante con protección para reducir la interferencia electromagnética.

SWITCH Un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro. Su empleo es muy común cuando existe el propósito de conectar múltiples redes entre sí para que funcionen como una sola. Un conmutador suele mejorar el rendimiento y seguridad de una red de área local.

TCP (Transmission Control Protocol), es uno de los protocolos de comunicaciones sobre los que se basa internet. Posibilita una comunicación libre de errores entre ordenadores en internet.

Telnet, es el protocolo estándar de Internet que permite la conexión a un terminal remoto.

TFTP son las siglas de Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial). Protocolo en internet para la carga remota de fichero en equipos embebidos.

Topología, disposición física de los nodos de una red. Por ejemplo, es posible que se encuentren formando un bus, una estrella, un anillo, etc.

Trama, conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado. Desde uno de los componentes de equipo de red, los cuadros pueden ser unidestinados (enviados a un solo dispositivo), multidestinados (enviados a dispositivos múltiples) o difundidos (enviados a todos los dispositivos).

UDP (UserDatagramProtocol), Protocolo de Datagrama de usuario.

UTP Par trenzado sin blindaje. Es un medio de transmisión de 4 pares de cable que se usa en una gran variedad de redes. UTP no requiere es espaciamiento fijo entre conexiones propio de las conexiones con cable coaxial. Hay 5 tipos de cableado UTP comúnmente utilizados: cableado categoría 1, cableado categoría 2, cableado categoría 3, cableado categoría 4, cableado categoría 5.

APORTES DE LA TESIS

A veces suele presentarse cierto recelo ante la innovación, los trabajadores a veces suelen mostrarse reacios a los cambios; pero así como hay cierta incredulidad a esta tecnología por algunos trabajadores del INABIF, es grato saber que también por otro lado hay expectativa por otros trabajadores que apuestan por este cambio.

Este proyecto es un muy buen aporte para una entidad del estado, porque sabemos que ellas en su limitado presupuesto; aunque quisieran a veces no pueden llevar a cabo proyectos, como es este, por si mismas. Para otras

instituciones con gran número de equipos de cómputo también será un aporte significativo, pues al tener redes afines entre ellas; podrán también tener como base a este proyecto para ser adecuado a sus organizaciones sin objeción alguna.

Los aportes generales de este proyecto son:

- Fluidez adecuada de la información a través de la red en la institución.
- Seguridad en los datos e información que se comparte dentro de la institución.
- Control del acceso y uso adecuado del internet por los usuarios en general.

2.4 MARCO METODOLOGICO

En esta parte se describen las fuentes de información, el tipo de investigación, así como también los métodos y herramientas por utilizar para la realización del presente trabajo.

FUENTES DE INFORMACIÓN

La fuente de información es el lugar donde se encuentran los datos requeridos, que posteriormente se pueden convertir en información útil para el investigador. Los datos son todos aquellos fundamentos o antecedentes que se requieren para llegar al conocimiento exacto de un objeto de estudio. Estos datos, que se deben

recopilar de las fuentes, tendrán que ser suficientes para poder sustentar y defender un trabajo (Eyssautier de la Mora, 2002).

FUENTES PRIMARIAS

Se refieren a aquellos portadores originales de la información que no han retransmitido o grabado en cualquier medio o documento la información de interés. Esta información de fuentes primarias la tiene la población misma. Para extraer los datos de esta fuente se utiliza el método de encuesta, de entrevista, experimental o por observación (Eyssautier de la Mora, 2002).

La recopilación de la información requerida para la elaboración de la propuesta de Plan de Proyecto para el diseño e implementación de redes virtuales en el INABIF, se estará llevando a cabo mediante entrevistas con los proveedores de soluciones tecnológicas afines y se invocará el juicio de expertos de los diferentes involucrados a nivel del área de redes y telecomunicaciones.

FUENTES SECUNDARIAS

Se refieren a todos aquellos portadores de datos e información que han sido previamente transmitidos o grabados en cualquier documento y utilizan el medio que sea. Esta información se encuentra a disposición de todo investigador que la necesite (Eyssautier de la Mora, 2002).

Para este fin se consultarán las páginas web de los principales proveedores tecnológicos, a partir de los cuales se obtendrá la información básica referente al tema que se desarrolla.

Adicionalmente, se utilizará la información que se dispone con las normativas técnicas vigentes, manuales y procedimientos que se manejan a nivel de redes y telecomunicaciones.

TECNICAS DE INVESTIGACION

INVESTIGACION MIXTA

Corresponde a trabajos de investigación en cuyo método de recopilación y tratamiento de datos se conjuntan la investigación documental con la de campo, con el propósito de profundizar en el estudio del tema propuesto para tratar de cubrir todos los posibles ángulos de explotación. Al aplicar ambos métodos se pretende consolidar los resultados obtenidos (Rodríguez, 2011)

Se hará uso de este tipo de investigación con la finalidad de obtener información sobre el diseño de redes virtuales y la propuesta técnica de las diferentes opciones de soluciones tecnológicas identificadas en el mercado. Además, por la necesidad existente de realizar un levantamiento de requerimientos técnicos funcionales para obtener un estado de la situación actual y fundamentar las propuestas de solución basado en la información que facilitarían los proveedores.

INVESTIGACION APLICADA TECNOLOGICA

La investigación aplicada tecnológica, o simplemente investigación tecnológica, se entendería como *aquella que genera conocimientos o métodos dirigidos al sector productivo de bienes y servicios, ya sea con el fin de mejorarlo y hacerlo más eficiente, o con el fin de obtener productos nuevos y competitivos en dicho sector* (irónicamente, las armas, bajo este marco, caerían dentro del sector "productivo" de "bienes" y "servicios"). Sus productos pueden ser prototipos y hasta eventualmente artículos científicos publicables. En el caso de la investigación médica que mencionábamos antes, la investigación tecnológica se realizaría alrededor del desarrollo de una droga específica para la cura de una determinada dolencia. Se pretendería, evidentemente en este caso, que la droga fuera a dar al mercado.

En el contexto que manejamos, *si la aplicación del conocimiento no buscara acceder al sector productivo, se consideraría, o bien ingeniería o bien investigación aplicada fundamental.* En este último caso podría considerarse, por ejemplo, el desarrollo de instrumentación sofisticada que coadyuvara a la solución de algún otro problema de investigación aplicada, como cierta instrumentación utilizada para las naves de investigación espacial; también en este caso caería el desarrollo de instrumentación para actividades astronómicas. Su desarrollo, por su complejidad, puede considerarse, per se, investigación aplicada fundamental y no debe considerarse, en el sentido que estamos manejando, como investigación tecnológica, pues no pretendería impactar, en el sector productivo. Este resultado, sin embargo, puede convertirse en una tecnología en el momento

que su dueño, la agencia espacial, o el observatorio, lo transfiera, o pretendiera transferirlo al sector productivo.

La investigación tecnológica, se ha hecho muy a menudo a partir de la investigación básica de punta. Es bien conocido el caso de Japón, país que, sobre todo en el comienzo de su recuperación de posguerra, ha aprovechado la investigación básica de otros países con ese fin. En otros casos, la investigación tecnológica se ha hecho con base en la aplicación de conocimientos relativamente divulgados, es decir ingenieriles; como un ejemplo de esto, podría mencionarse la computadora personal o la mejora de procesos en la planta industrial.

Todavía, podría hacerse otra catalogación más, la de investigación científica académica, que sería la actividad que engloba tanto la investigación pura como la investigación aplicada básica cuando ésta se realiza en recintos universitarios.

METODO DE INVESTIGACION

El método es la ruta que se sigue en las ciencias para alcanzar un fin propuesto y la metodología el cuerpo de conocimiento que describe y analiza los métodos para el desarrollo de una investigación. Ambos se han particularizado y son objeto de un tratamiento especial de acuerdo con cada ciencia particular (Eyssautier de la Mora, 2002).

A continuación, se describe el método de investigación a utilizar para este trabajo.

METODO ANALITICO – SINTETICO

El método analítico es la observación y examen de hechos. Este método distingue los elementos de un fenómeno y permite revisar ordenadamente cada uno de ellos por separado, para luego establecer leyes universales (Rodríguez, 2011).

La síntesis es la meta y resultado final del análisis. El método sintético no es propiamente un método de investigación, sino una operación fundamental por medio de la cual se logra la comprensión de la esencia de lo que se ha conocido en todos sus componentes particulares (a partir del análisis). Este proceso relaciona hechos aparentemente aislados y formula una teoría que unifica los diversos elementos.

Con la aplicación de este método, se pretende realizar un análisis de la situación presentada actualmente, desde la perspectiva técnica y considerar los requerimientos asociados a las nuevas tecnologías de soluciones existentes que proponen ser la base primordial para lograr los lumbrales de servicio esperados.

HERRAMIENTAS

JUICIO DE EXPERTOS

Es un conjunto de opiniones que pueden brindar profesionales expertos en una industria o disciplina, relacionadas al proyecto que se está ejecutando. Este tipo de información puede ser obtenida dentro o fuera de la organización, en forma gratuita o por medio de una contratación, en asociaciones profesionales, cámaras de comercio, instituciones gubernamentales, universidades. (Wordpress).

Este proyecto por tener tanta connotación técnica, es un hecho que la aplicación de esta herramienta no se puede obviar y la experiencia de todas las personas que se desenvuelven en áreas afines resulta ser insumo relevante para la conformación y desarrollo de la propuesta.

SOFTWARE

Se utilizará todo el Software disponible en el tema de simulación de Redes (**Cisco Packet Tracer, GNS3**) Y también el **Sniffer** para registrar la actividad realizada por los ordenadores.

ENTREVISTA A LOS INVOLUCRADOS

Se harán entrevistas a los involucrados en este proyecto, principalmente para definir el alcance del proyecto, levantar el listado de requerimientos técnicos, obtener el juicio de experto y poner en práctica recomendaciones de técnicas y profesionales involucrados en el estudio de mercado. Entre los involucrados están:

- Funcionario del Departamento de Redes y Telecomunicaciones
- Funcionario del Departamento de Seguridad Informática
- Usuarios de la red.

CAPITULO III: DESARROLLO DE LA IMPLEMENTACION

3.1 CRITERIOS PARA LA IMPLEMENTACION

De acuerdo a los lineamientos de desarrollo que queremos alcanzar para un correcto diseño lógico, nos basamos en 4 criterios fundamentales.

- Seguridad.
- Funcionalidad.
- Escalabilidad.
- Adaptabilidad.

El objetivo principal es mejorar el Rendimiento y Seguridad de la plataforma LAN que soporta los procesos de la institución, para ello los cuatro criterios serán pilares para esta propuesta.

a) Seguridad

- ACL,
- Se aplicará la instalación de un Firewall

b) Funcionalidad

La red proporciona conectividad de usuario a usuario a través de la red, y de usuario a aplicación con una velocidad y confiabilidad muy razonable.

- VLAN
- La red actual

c) Escalabilidad

La red podrá aumentar su tamaño sin que ello produzca cambios importantes en el diseño general por lo que se proveerá de un número considerable de puntos de red. Los switches son escalables para permitir aumentar la cantidad de puertos para soportar crecimientos futuros.

d) Adaptabilidad

La red estará diseñada teniendo en cuenta las diferentes tecnologías y sus diferentes aplicaciones normativas lo que garantizará una amplia adaptabilidad muy independiente de la tecnología que se llegue a implementar.

3.2 DISEÑO DE LA ESTRUCTURA LOGICA

De acuerdo con el MOF de la institución elaboramos un inventario general de Usuarios por cada área.

- **Para la Unidad Administrativa.**

Tabla 3.1: Inventario de usuarios de la Unidad Administrativa

CARGO DEL USUARIO EN LA INSTITUCION		SERVICIO Y APLICACIONES QUE USA												
		Internet	Correo	FTP	Intranet	SICUANEC	Existencias	SISCAR	SISUGPI	Alimentos	SIGIT	SIRFAM	Voluntariad	SISBEN
Gerente de Unidad Administrativa	PCA-1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Especialista Administrativo (2)	PCA-2 y 3	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		
Tco Administratico Secretarial (3)	PCA - 4 al 6	✓	✓		✓	✓	✓	✓	✓					
Operadora de central Telefónica	PCA - 7	✓	✓											
Auxiliar Administrativo (2)	PCA - 8 y 9	✓	✓						✓					
Jefe del Trabajo de Contabilidad	PCA - 10	✓	✓	✓	✓		✓							
Especialista Admin Contabilidad (8)	PCA - 11 al 18	✓	✓	✓	✓		✓							
Jefe del Equipo de Logistica	PCA - 19	✓	✓	✓	✓	✓	✓		✓	✓				
Especialista Admin Logistica (9)	PCA - 20 al 28	✓	✓	✓	✓	✓	✓			✓				
Técnico Aministrativo (8)	PCA - 29 al 36	✓	✓	✓			✓							
Auxiliar Administrativo - Logística (2)	PCA - 37 y 38	✓	✓				✓							
Jefe del Equipo de Recursos Humanos	PCA - 39	✓	✓	✓	✓			✓						
Especialista Administrativo (3)	PCA - 40 al 42	✓	✓	✓	✓									
Trabajador Social	PCA - 43	✓	✓				✓							
Técnico Aministrativo (3)	PCA - 44 al 46	✓	✓											
Jefe del Equipo de Sistemas	PCA - 47	✓	✓	✓	✓	✓	✓	✓	✓	✓				
Especialista en Informática (3)	PCA - 48 al 50	✓	✓	✓	✓	✓	✓							
Técnico en Informática (2)	PCA - 51 y 52	✓	✓		✓									
Especialista Administrativo	PCA - 53	✓	✓	✓										
Técnico Administrativo (3)	PCA - 54 al 56	✓	✓											

FUENTE: Elaboración propia

- **Para la unidad de Planeamiento y Resultados:**

Tabla 3.2: Inventario de usuarios de la Unidad de Planeamiento y Resultados.

CARGO DEL USUARIO EN LA INSTITUCION		SERVICIO Y APLICACIONES QUE USA												
		Internet	Correo	FTP	Intranet	SICUANEC	Existencias	SISCAR	SISUGPI	Alimentos	SIGIT	SIRFAM	Voluntariad	SISBEN
Gerente de Unidad	PCP - 1	√	√	√	√	√	√		√		√			√
Tco Administratico Secretarial (3)	PCP - 2 al 4	√	√		√									√
Equipo de Trabajo de Planificación: Especialista Administrativo (3)	PCP - 5 al 7	√	√	√	√	√	√							
Equipo de Trabajo de Presupuesto: Especialista Administrativo (3)	PCP - 8 al 10	√	√	√	√	√	√							
Equipo de Trabajo de Seguimiento y Evaluación: Especialista Administrativo (3)	PCP - 11 al 13	√	√	√	√									
Equipo de Trabajo de Racionalización: Especialista Administrativo (3)	PCP - 14 al 16	√	√	√	√	√	√							

FUENTE: Elaboración propia.

- **Para la Unidad Gerencial de Desarrollo Integral de la Familia y Promoción del Voluntariado**

Tabla 3.3 Inventario de usuarios de la Unidad Gerencial de Desarrollo Integral de la Familia y Promoción del Voluntariado.

CARGO DEL USUARIO EN LA INSTITUCION		SERVICIO Y APLICACIONES QUE USA												
		Internet	Correo	FTP	Intranet	SICUANEC	Existencias	SISCAR	SISUGPI	Alimentos	SIGIT	SIRFAM	Voluntariad	SISBEN
Gerente de Unidad	PCDF - 1	√	√	√	√	√	√	√	√	√	√		√	√
Asistete de Gerencia	PCDF - 2	√	√	√	√	√	√				√		√	
Asistente Administrativo	PCDF - 3	√	√	√	√								√	
Técnico Administrativo Secretarial	PCDF - 4	√	√		√								√	
Técnico Administrativo	PCDF - 5	√	√	√									√	
Jefe de Promoción del Voluntariado	PCDF - 6	√	√		√								√	
Director del Equipo de Trabajo de CEDIF	PCDF - 7	√	√		√		√	√					√	
Trabajador Social (4)	PCDF - 8 al 11	√	√		√		√							
Psicólogo (5)	PCDF - 12 al 16	√	√		√									
Asistente Administrativo (4)	PCDF - 17 al 20	√	√		√									
Técnico Administrativo (5)	PCDF - 21 al 25	√	√											
Especialistas Sociales (4)	PCDF - 26 al 29	√	√		√		√						√	
Nutricionista (2)	PCDF - 30 Y 31	√	√		√		√			√				

FUENTE: Elaboración propia.

- **Para la Unidad Gerencial de Protección Integral**

Tabla 3.4 Inventario de usuarios de la Unidad Gerencial de Protección Integral.

CARGO DEL USUARIO EN LA INSTITUCION		SERVICIO Y APLICACIONES QUE USA												
		Internet	Correo	FTP	Intranet	SICUANEC	Existencias	SISCAR	SISUGP	Alimentos	SIGIT	SIRFAM	Voluntariad	SISBEN
Gerente de Unidad	PCPI - 1	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		
Asistente Administrativo	PCPI - 2	✓	✓	✓	✓	✓	✓					✓		
Técnico Administrativo Secretarial	PCPI - 3	✓	✓	✓	✓									
Psicólogo (15)	PCPI - 4 al 18	✓	✓	✓	✓									
Trabajador Social (10)	PCPI - 19 al 28	✓	✓	✓	✓				✓			✓		
Nutricionista	PCPI - 29	✓	✓		✓		✓			✓				
Enfermera (4)	PCPI - 30 al 33	✓	✓		✓									
Asistente Administrativo (4)	PCPI - 34 al 37	✓	✓	✓	✓									
Técnico en Enfermería (5)	PCPI - 38 al 42	✓	✓											
Técnico Administrativo (5)	PCPI - 43 al 47	✓	✓	✓										
Especialistas Sociales (13)	PCPI - 48 al 60	✓	✓	✓	✓		✓							
Médico	PCPI - 61	✓	✓	✓	✓									
Coordinador	PCPI - 62	✓	✓	✓	✓		✓		✓					

FUENTE: Elaboración propia.

- **Para la Unidad Gerencial de Investigación Tutelar.**

Tabla 3.5Inventario de usuarios de la Unidad Gerencial de Investigación Tutelar

CARGO DEL USUARIO EN LA INSTITUCION		SERVICIO Y APLICACIONES QUE USA												
		Internet	Correo	FTP	Intranet	SICUANEC	Existencias	SISCAR	SISUGPI	Alimentos	SIGIT	SIRFAM	Voluntariad	SISBEN
Gerente de Unidad	PCIT - 1	✓	✓	✓	✓	✓		✓			✓	✓	✓	
Técnico Administrativo Secretarial	PCIT - 2	✓	✓	✓	✓			✓			✓			
Director	PCIT - 3	✓	✓	✓	✓			✓			✓			
Especialistas Sociales (5)	PCIT - 4 al 8	✓	✓	✓	✓						✓			
Abogado (6)	PCIT - 9 al 14	✓	✓	✓	✓						✓			
Trabajador Social (2)	PCIT - 15 y 16	✓	✓	✓	✓						✓			
Psicólogo (3)	PCIT - 17 al 19	✓	✓	✓	✓				✓					

FUENTE: Elaboración propia.

- **Para la Unidad Gerencial para el Desarrollo de la Población e Riesgo**

Tabla 3.6 Inventario de usuarios de la Unidad Gerencial para el Desarrollo de la Población en Riesgo

CARGO DEL USUARIO EN LA INSTITUCION		SERVICIO Y APLICACIONES QUE USA												
		Internet	Correo	FTP	Intranet	SICUANEC	Existencias	SISCAR	SISUGP	Alimentos	SIGIT	SIRFAM	Voluntariad	SISBEN
Gerente de Unidad	PCDP - 1	√	√	√	√	√	√		√	√	√	√	√	√
Asistente de Gerencia	PCDP - 2	√	√	√	√	√						√	√	√
Técnico Administrativo Secretarial	PCDP - 3	√	√	√	√									√
Especialista Administrativo (2)	PCDP - 4 y 5	√	√	√	√									√
Especialista en Comunicación	PCDP - 6	√	√	√	√									√
Abogado (3)	PCDP - 7 al 9	√	√	√	√				√					√

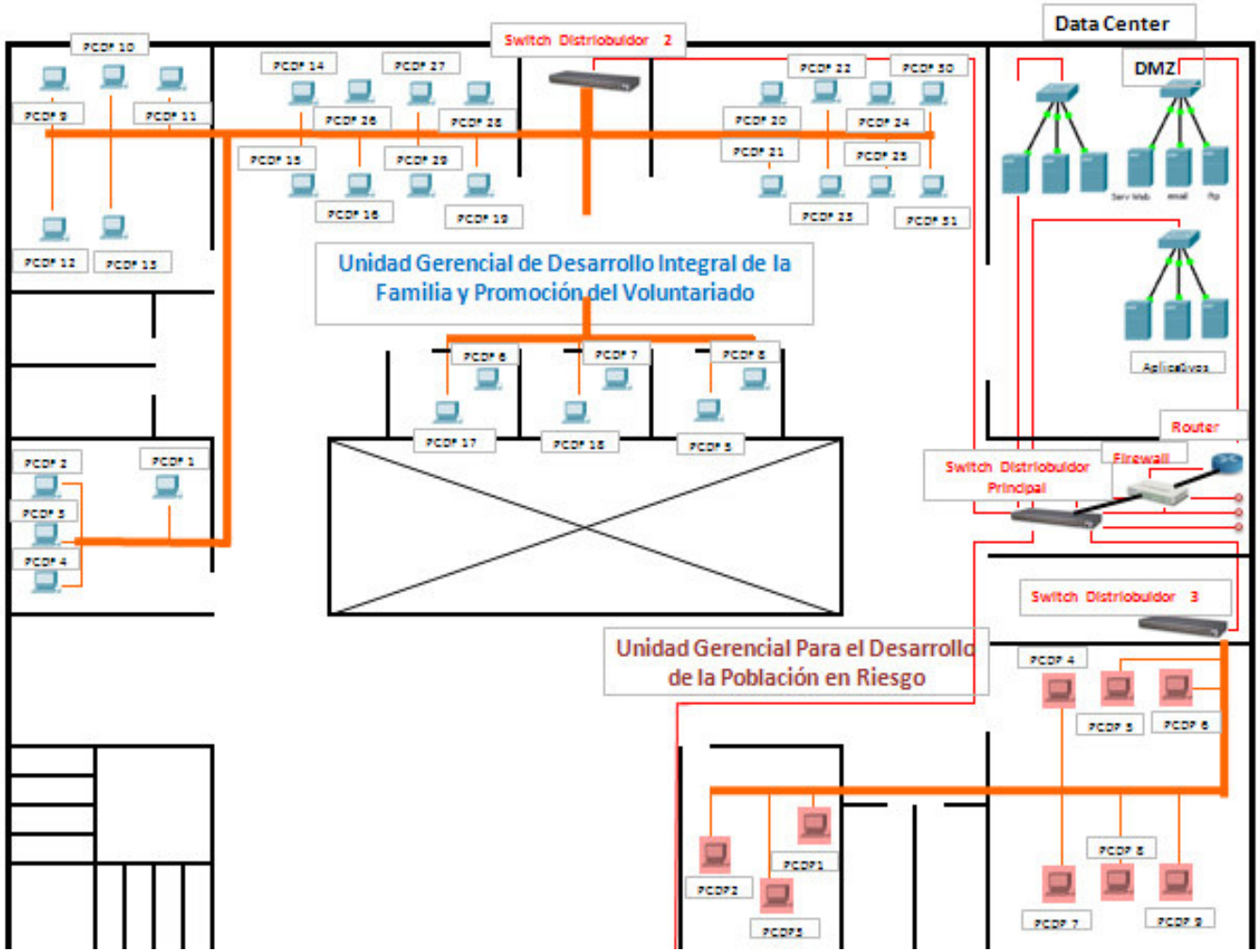
FUENTE: Elaboración propia.

La elaboración de estos inventarios sirvió para hacer un análisis profundo de la interacción de usuarios y dispositivos de la red; lográndose establecer que la mejor manera de segmentar la red es por áreas; es decir, se debe crear una Vlan para cada área de la institución.

3.3 TOPOLOGIA DE RED DE LA INSTITUCION.

Piso 3 - a

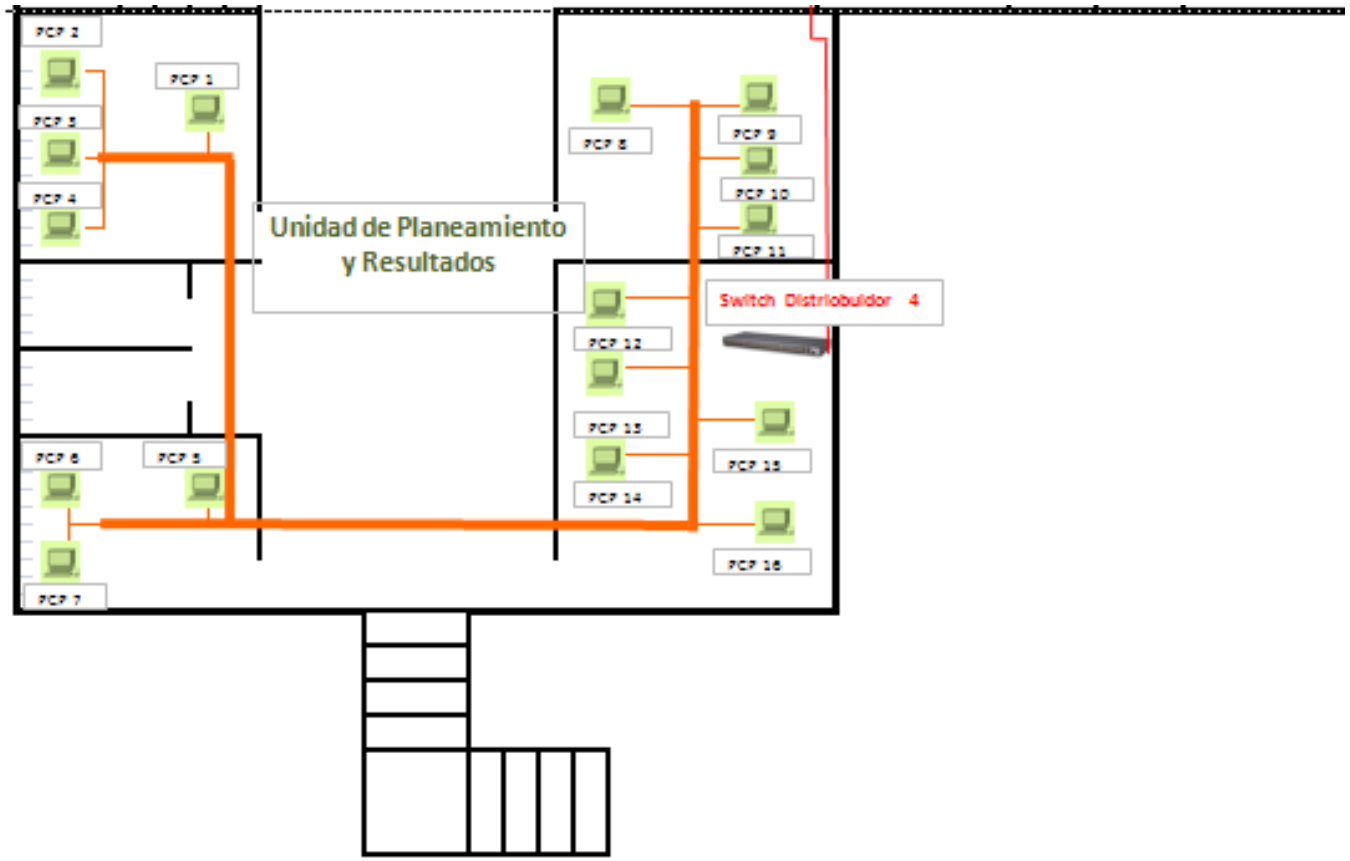
Figura 2.25 Topología de red Piso 3-a



FUENTE: Elaboración propia

Piso 3 –b

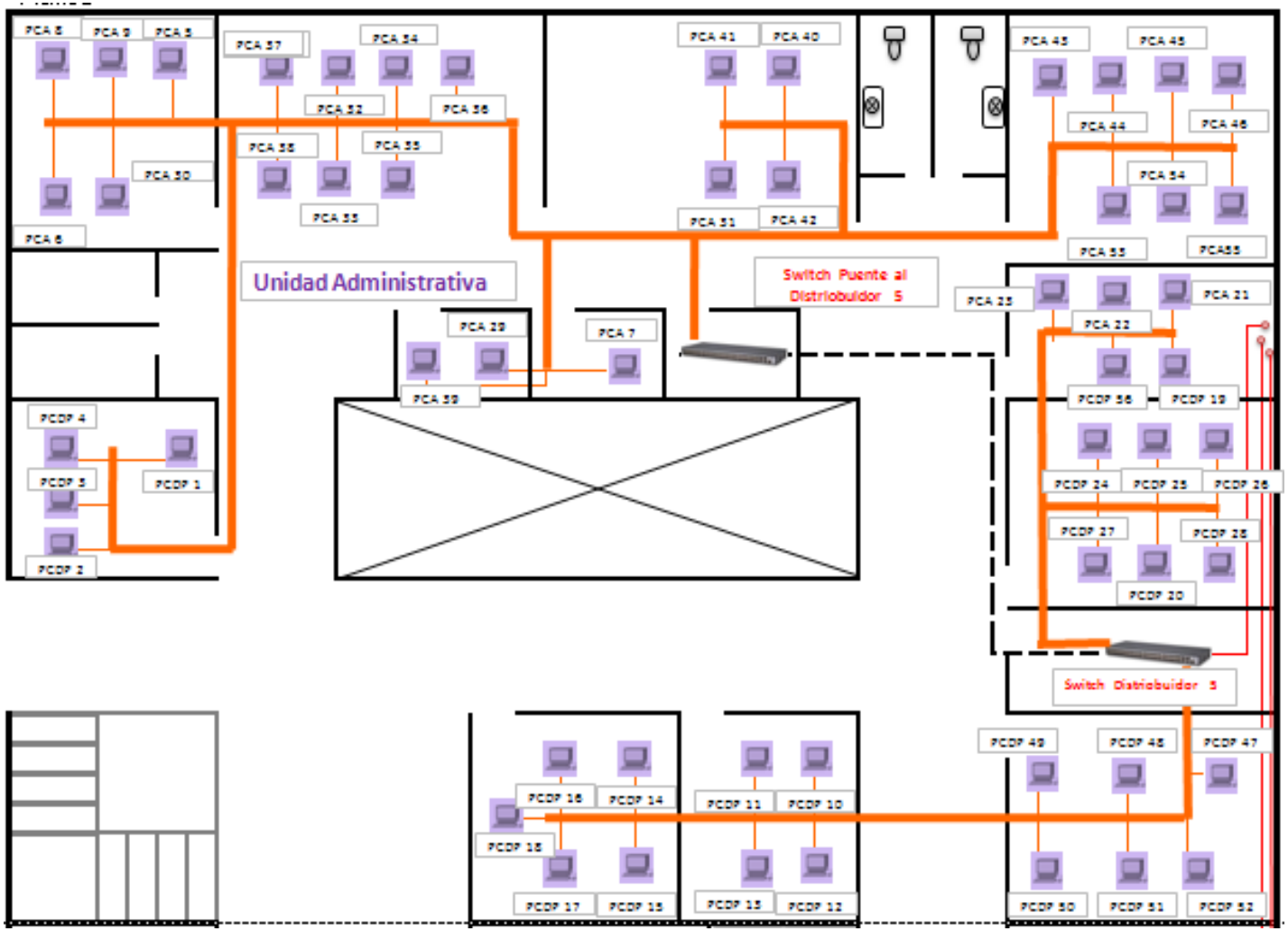
Figura 3.2: Topología de red Piso 3-b



FUENTE: Elaboración propia

Piso 2 –a

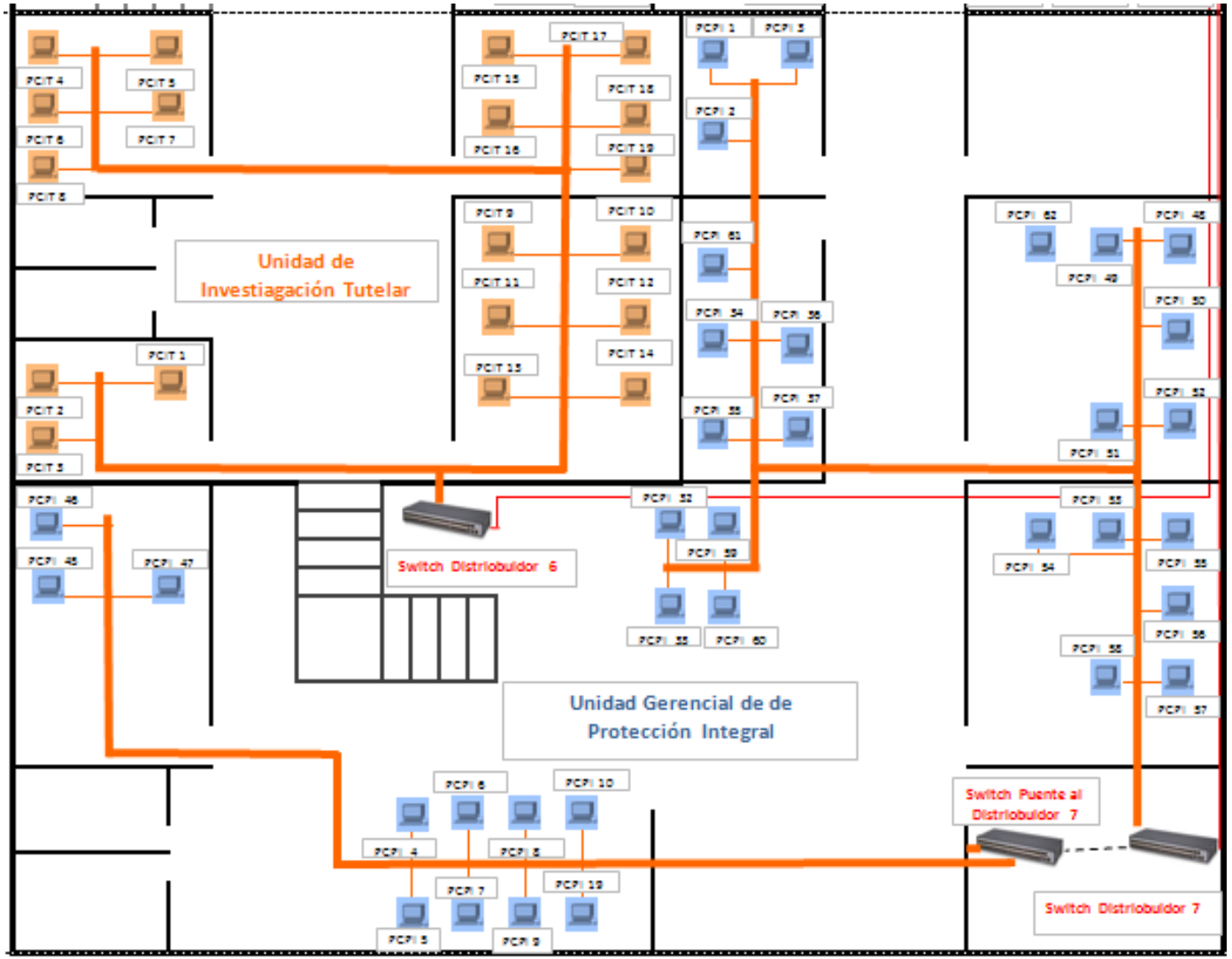
Figura 3.3: Topología de red Piso 2-a



FUENTE: Elaboración propia

Piso 2 – b

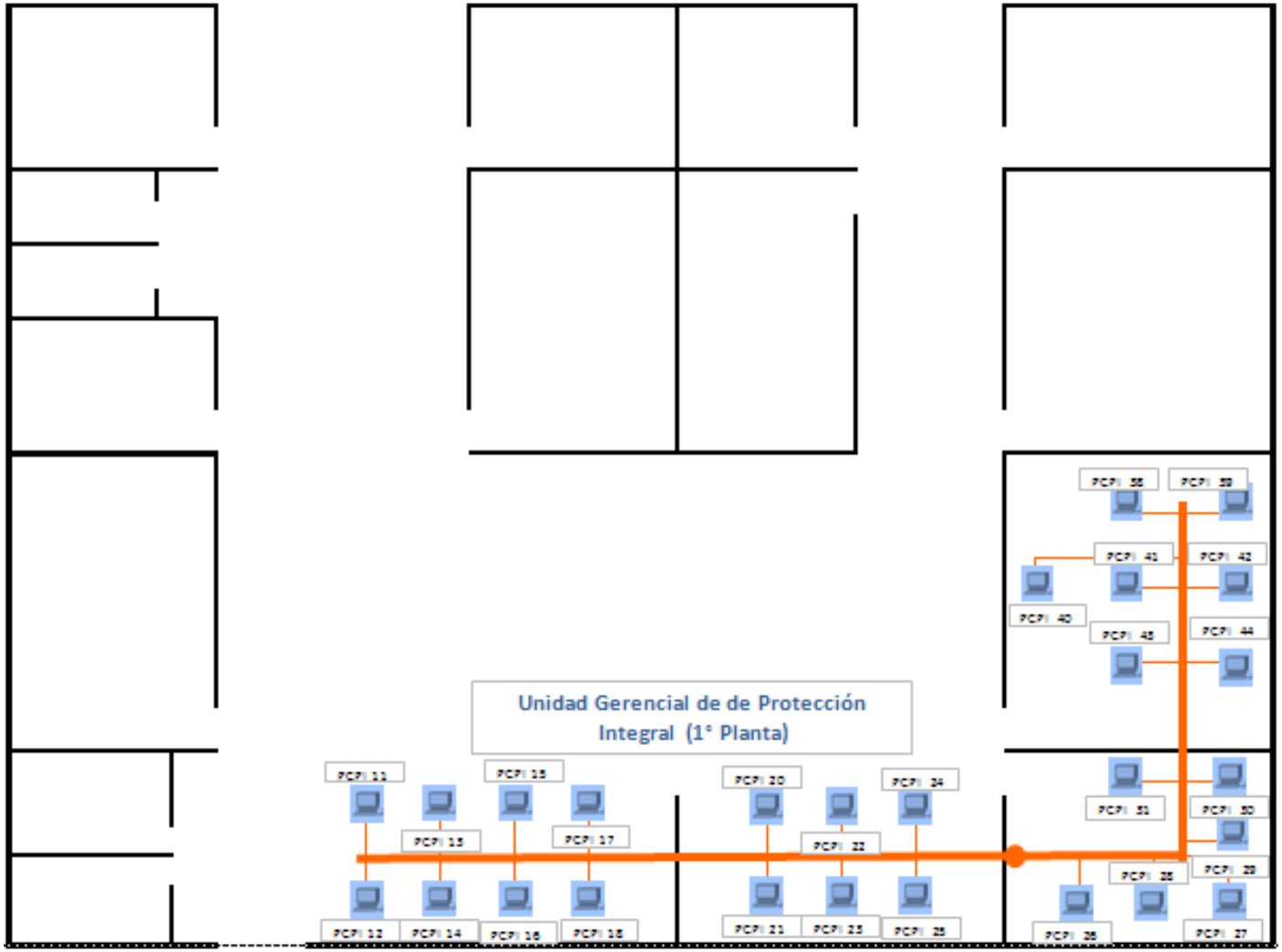
Figura 3.4: Topología de red Piso 2-b



FUENTE: Elaboración propia

Piso 1

Figura 3.5: Topología de red Piso 1



FUENTE: Elaboración propia

3.4 CONFIGURACION DE DISPOSITIVOS

- El **switch HP V1905** que posee la institución es un dispositivo que permite crear hasta 64 Vlan. Nosotros solo crearemos 7, con la siguiente asignación de puertos:

Figura 3.6: Asignación de puertos en el switch

FUENTE: Elaboración propia

- El **firewall Fortinet 200B poe** de la institución es capaz de administrar mediante Listas de Acceso. Debido a que nuestra segmentación es por áreas, se presentan muchas excepciones, para esto nos ayudaremos de este dispositivo.

1Figura 3.7 Firewall Fortinet 200B poe

Tabla 3.7 Control de lista acceso

CONTROL DE LISTAS DE ACCESO
FIREWALL Fortinet 200B poe

		WAN		LAN						DMZ	
Red		Entrada	Salida	Entrada	Salida					Entrada	Salida
					R1	R2	R3	R4	R5	R6		
DMZ	191.160.1.0/24	P	P	P *	D *	P	D *	D *	P	D *	-	-
LAN	VLAN A: 190.160.1.0/24	P	P	-	-	D *	D *	D *	D *	D *	P *	P *
	VLAN P: 190.160.2.0/24	P	P	-	D *	D *	D *	D *	D *	D *	P	P
	VLAN DF: 190.160.3.0/24	P	P	-	D *	D *	-	D *	D *	D *	P *	P *
	VLAN PI: 190.160.4.0/24	P	P	-	D *	D *	D *	-	D *	D *	P *	P *
	VLAN IT: 190.160.5.0/24	P	P	-	D *	D *	D *	D *	-	D *	P	P
	VLAN DP: 190.160.6.0/24	P	P	-	D *	D *	D *	D *	D *	-	P *	P *
WAN	192.168.1.2/24	-	-	P	P	P	P	P	P	P	P	P

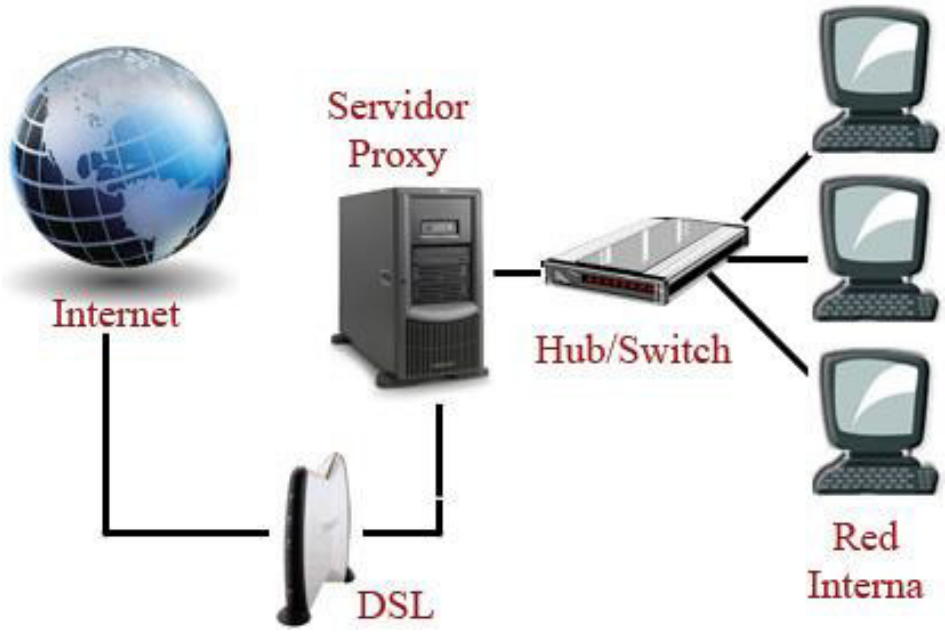
R1: VLAN A
R2: VLAN P
R3: VLAN DF
R4: VLAN PI
R5: IT
R6: DP

P : Permitir
D: Denegar
* : Con resitricciones

SERVIDOR PROXI

Un Servidor proxi es un equipo intermediario situado entre el sistema del usuario e internet. Puede utilizarse para registrar el uso del internet y también para bloquear el acceso a una sede web.

Figura 3.8 Diagrama del funcionamiento de un Servidor Proxi.



FUENTE: http://cinthyapaolacordova.edublogs.org/%C2%BF-que-es-un-servidor-proxy/

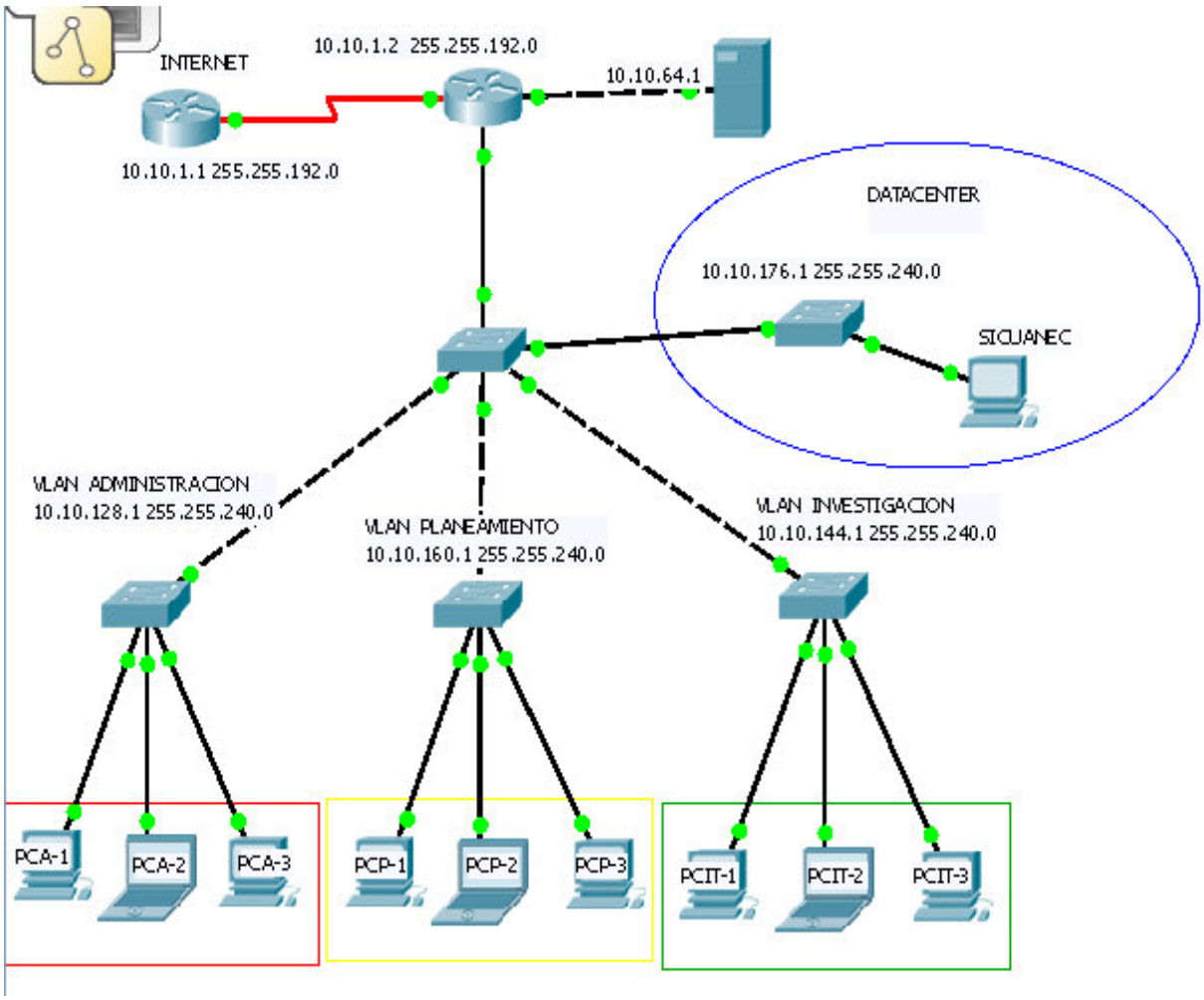
Configuramos un servidor proxi para bloquear algunas páginas Web por diversas razones, las que se sustenta en el estudio y análisis del MOF de la institución.

Se establece horarios de acceso a las páginas de redes sociales, You Tube y otros para algunos trabajadores sólo en horarios de refrigerio.

3.5 SIMULACION DE LA RED EN EL SIMULADOR CISCO PACKET TRACER.

Para comprobar la correcta segmentación de la red y el parcial funcionamiento de las Vlans utilizamos el Cisco Packet Tracer.

Figura 3.9: Topología en Cisco Packet Tracer



2FUENTE: Elaboración propia

CAPITULO IV: ANALISIS DE COSTOS Y BENEFICIOS

4.1 ANALISIS DE COSTO

Tabla 4.1: Costos de Operaciones.

COSTOS DE OPERACIONES				
Descripción	Cantidad	Unidad de medida	Precio unitario	Precio Parcial
Elaboración y aprobación de Tesis				**370**
Elaboración				345
Asesoría	3	sesión	50	150
Servicio de Internet	2	meses	80	160
Impresiones	0.35	millar	100	35
Aprobación				25
Pago por resolución	1	pago	25	25
Recopilación y revisión bibliográfica				**204**
Investigación de campo				132
Libro de portal web	2	Unidad	25	50
Libro "Redes de Computadoras"	1	Unidad	45	45
Libro CCNA Exploration	1	Unidad	62	62
Revisión bibliográfica				72
Servicio de Internet	2	meses	36	72
Análisis y especificación de requerimientos				**225**
Entrevista con usuarios de la red	5	evento	25	125
Servicio de Internet	2	meses	30	60
Impresión	0.4	millar	100	40
Plan del Proyecto				**272**
Definición de metodología aplicada	1	acción	30	30
Identificación de requerimientos	4	acción	30	120
Asesorías	1	sesión	50	50
Servicios de Internet	2	meses	36	72
Diseño de topología				**450**
Especificar requerimientos	4		30	120
Diseño de topología	5		40	200
Asesorías	1		50	50
Servicio de Internet	2		40	80

Implementación				**2030**
Elaboración de inventario de usuarios	1	accion	40	40
Control de Listas de Acceso	1	accion	40	40
Determinación de restricciones	1	accion	30	30
Configuración de Switch principal	1	accion	400	400
Configuración de Firewall	1	accion	500	500
Configuracion de Pcs	340	accion	3	1020
Capacitacion				**600**
Capacitación de usuarios	6	evento	100	600
Elaboración del informe de tesis				**40**
Impresión	1	millar	30	30
Estampado y acabados	1	unidad	10	10
Gastos generales				**8498**
Personal				**7000**
Tesista	7	meses	1000	7000
Equipo				**426**
Computadora - Software de oficina	7	meses	58	406
Testeador	2	meses	10	20
Servicios				**1072**
Servicio de comunicaciones	7	unidad	26	182
Viáticos diversos	7	meses	30	210
Imprevistos	1	unidad	400	400
Agua, Luz y Renta	5	meses	40	200
Accesorios de oficina	2	meses	40	80
TOTAL				**S/. 12,689.00**

FUENTE: Elaboración propia.

4.2 ANALISIS DE BENEFICIO

Tabla 4.2 Beneficio Económico

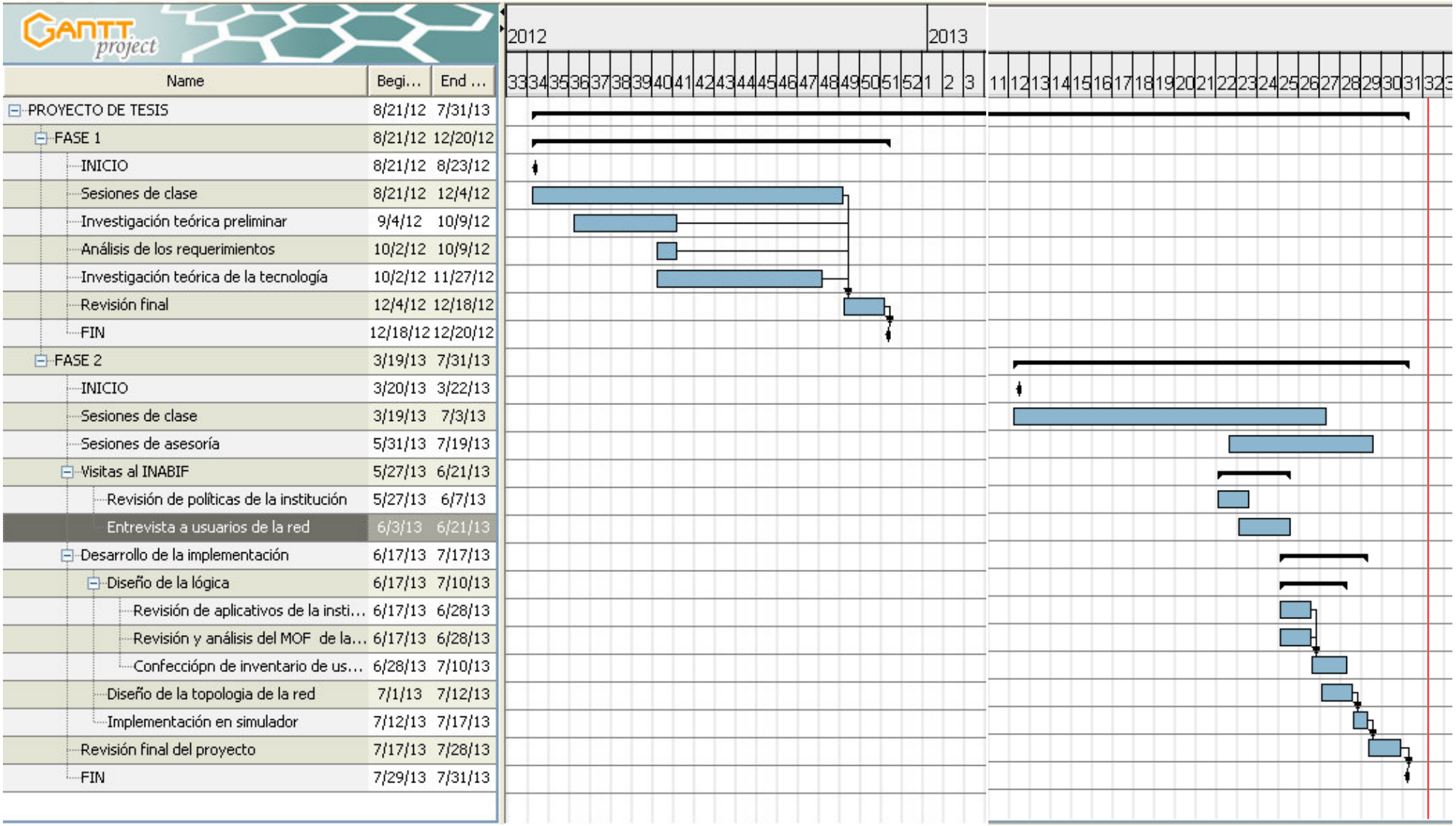
BENEFICIO ECONÓMICO	meses				
TIPOS DE BENEFICIOS	1	2	3	4	5
Incremento de productividad mens (4%; 8% y 10%)del personal (sueldo prom 1500 por 50 emp)	3000	6000	7500	7500	7500
Ahorro por actualizaciones	300	300	300	300	300
Ahorro de dinero, con la eliminarcion del papel	40	40	40	40	40
Beneficio total	3340	6340	7840	7840	7840

FLUJO MENSUAL	meses					
Descripcion	0	1	2	3	4	5
Beneficios		3,340	6,340	7,840	7,840	7,840
Egresos	S/. 12,689.00	S/. 100.00	S/. 100.00	S/. 100.00	S/. 100.00	S/. 100.00
Inversion	S/. 12,689.00					
Mantenimiento		100	100	100	100	100
Sumatoria I-E	S/. -12,689.00	S/. 3,240.00	S/. 6,240.00	S/. 7,740.00	S/. 7,740.00	S/. 7,740.00

VAN	S/. 18,408.88
TIR	36%
COSTO CAPITAL (TEM 20%)	1.53%

FUENTE: Elaboración propia

4.3 CRONOGRAMA DE ACTIVIDADES.



Name	Begi...	End ...
PROYECTO DE TESIS	8/21/12	7/31/13
FASE 1	8/21/12	12/20/12
INICIO	8/21/12	8/23/12
Sesiones de clase	8/21/12	12/4/12
Investigación teórica preliminar	9/4/12	10/9/12
Análisis de los requerimientos	10/2/12	10/9/12
Investigación teórica de la tecnología	10/2/12	11/27/12
Revisión final	12/4/12	12/18/12
FIN	12/18/12	12/20/12
FASE 2	3/19/13	7/31/13
INICIO	3/20/13	3/22/13
Sesiones de clase	3/19/13	7/3/13
Sesiones de asesoría	5/31/13	7/19/13
Visitas al INABIF	5/27/13	6/21/13
Revisión de políticas de la institución	5/27/13	6/7/13
Entrevista a usuarios de la red	6/3/13	6/21/13
Desarrollo de la implementación	6/17/13	7/17/13
Diseño de la lógica	6/17/13	7/10/13
Revisión de aplicativos de la insti...	6/17/13	6/28/13
Revisión y análisis del MOF de la...	6/17/13	6/28/13
Confecciópn de inventario de us...	6/28/13	7/10/13
Diseño de la topologia de la red	7/1/13	7/12/13
Implementación en simulador	7/12/13	7/17/13
Revisión final del proyecto	7/17/13	7/28/13
FIN	7/29/13	7/31/13

CONCLUSIONES:

- Luego de haber aprendido los diferentes conceptos, tanto en redes de información, como en seguridad, y otros más, en la carrera de Ingeniería de Sistemas e Informática, es necesario recalcar que fueron de sustancial ayuda para poder realizar el diseño y la implementación del presente proyecto, puesto que se ha fortalecido la parte teórica de los estudios con la experiencia y parte técnica en el ámbito laboral.

- Cada Vlan utiliza un dominio de broadcast, por lo que el tráfico de todo este dominio es independiente, con esto se elimina el riesgo de que un enlace que no pertenece al dominio de una Vlan en particular afecte los enlaces de otras Vlans.

- El diseño propuesto puede tener cambios previo cambio en la implementación debido a la escalabilidad de la tecnología con la que cuentan los equipos, por lo tanto, da la apertura de crecimiento en servicios.

- Una implementación de redes virtuales es vital dentro de las empresas que desean aumentar la productividad al mismo tiempo que reduce los costos de operación.

- El análisis de las tecnologías actuales justifica la migración hacia redes virtuales.

- Para formar las Vlans no es necesario tener equipos de las mismas características, pero si es necesario que trabajen con el mismo protocolo, es decir, con **802.1q** que es el estándar para formar las Vlans, esto hace que para formar redes Vlans no se deba utilizar un solo tipo de equipos de acuerdo al fabricante, sino que se pueda utilizar varios modelos de equipos y de diferentes marcas.

RECOMENDACIONES.

- Es recomendable incluir este tipo de infraestructuras de red a empresas públicas donde existen marcadamente grupos de trabajo.

- Es recomendable ampliar los contenidos académicos, en las facultades de Ingeniería de Sistemas, tópicos relacionados a Redes Virtuales.

- Es recomendable que el INABIF al momento de implementar este diseño documente cada uno de los procesos realizados para tener sustento en posibles actualizaciones del esquema de red.

- Controlar que la implementación de los equipos y servidores este acorde a lo diagramado en el diseño de red propuesta con el fin de sustentar lo antes dicho sobre los beneficios que ofrece esta implementación.

Referencias

Alcocer, C. (2000). *Redes de computadoras*. Lima: PUCP

Barceló, J. M., Iñigo, J., Marti, R., Olivé, E. y Perramon, X. (2004). *Redes de computadoras*. Cataluña: UOC

Delgado, H. H. (2009). *CCNA Exploration*. Lima: Macro

Eyssautier de la Mora, M. (2002). *Metodología de la investigación*. México: Cengage Learning.

Llano, E. (1993). *Telecomunicaciones y teleproceso* (2ª ed.). México: Exa Ingeniería

Milton, T. L. (2005). *Implementación de VLANS en la red de Telconet para una interconexión segura entre las agencias y la matriz de una institución bancaria* (Tesis de grado). Recuperado de https://bibdigital.epn.edu.ec/bitstream/15000/166/1/CD-0189.pdf

Molina, J. E. (2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la empresa editora y el comercio planta norte* (Tesis de grado). Recuperado de https://core.ac.uk/download/pdf/71999987.pdf

Rodríguez, D. (2011). *Metodología de la investigación*, Cataluña: UOC

Tanenbaum, A. (2003). *Redes de computadoras*. México: Pearson Education

ANEXOS.

APLICATIVOS USADOS EN EL INABIF

Figura Interfaz del Intranet INABIF

FUENTE: www.inabif.gob.pe

Figura Interfaz de Existencias INABIF

FUENTE: www.inabif.gob.pe

Figura Interfaz de Voluntariado del INABIF

FUENTE: www.inabif.gob.pe

Figura Interfaz de Sirfarm del INABIF

FUENTE: www.inabif.gob.pe

Figura Interfaz de Sisben

FUENTE: www.inabif.gob.pe

BANDWIDTH CONTROLLER STANDARD.

El Bandwith Controller Standard es una herramienta muy útil para distribuir de forma eficiente los recursos de red. Se emplea fundamentalmente para signar un volumen de datos específico para cada programa, servicio o conexión.

Esta herramienta utiliza un sistema de reglas que permite filtrar el tráfico mediante diversos parámetros. Hace posible un control efectivo de cada dispositivo de red de forma independiente. De esta forma, permite limitar el tráfico de internet sin afectar al de la red local.

Por otro lado, ofrece la posibilidad de supervisar la velocidad de descarga y la de subida, así como establecer 'puntos finales' a los que no accederá la conexión.

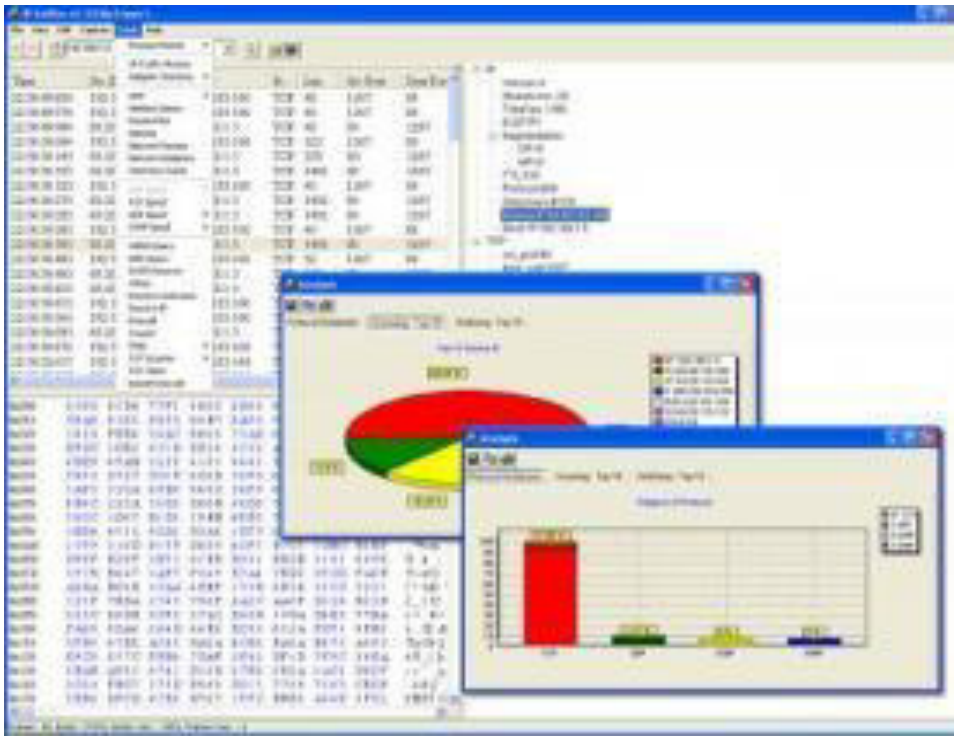
Otros parámetros interesantes son: filtrar por protocolo, usuario, dirección IP y MAC, Etc.

SNIFFER – Analizador de paquetes de Red

El Sniffer es un analizador de paquetes de red que captura las tramas de una red de computadoras. Este programa registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

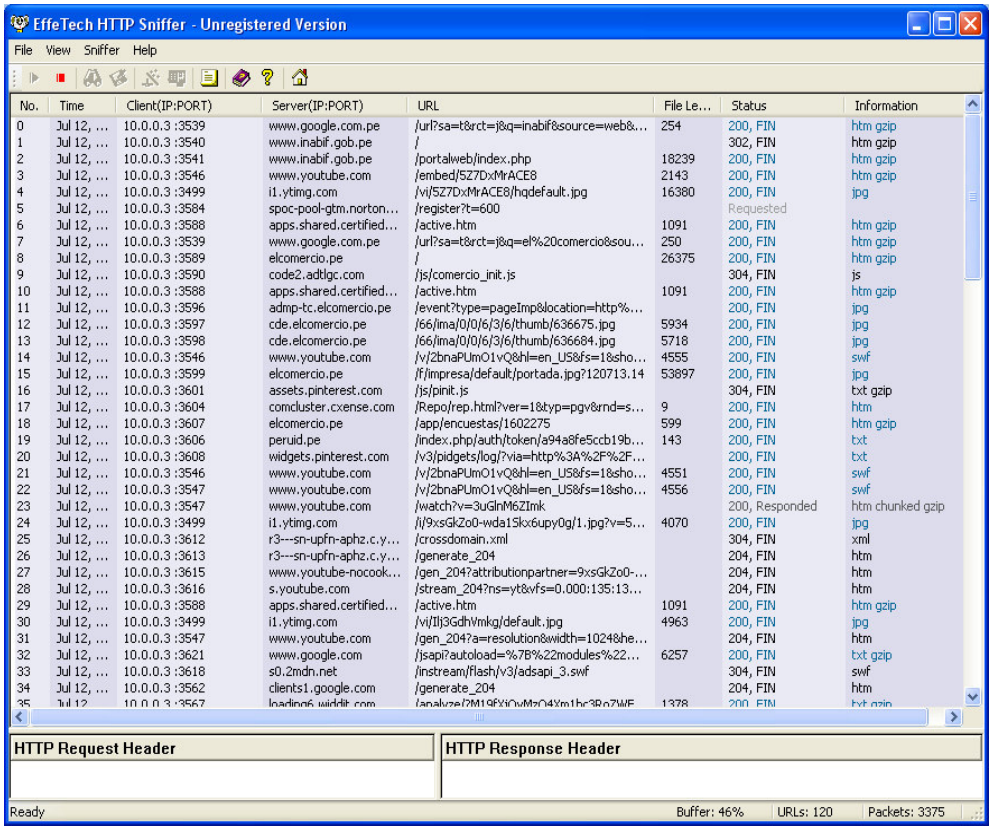
- Para determinar el porcentaje de beneficio con la implementación de las Vlans nos hemos ayudado de este programa.

Figura Interfaz del Sniffer



3FUENTE: Elaboración propia

Figura Ejecución del Sniffer



FUENTE: Elaboración propia

Figura Reporte en el Sniffer

EffeTech HTTP Sniffer - URL List - Only first 10 lines will be saved for unregistered user!

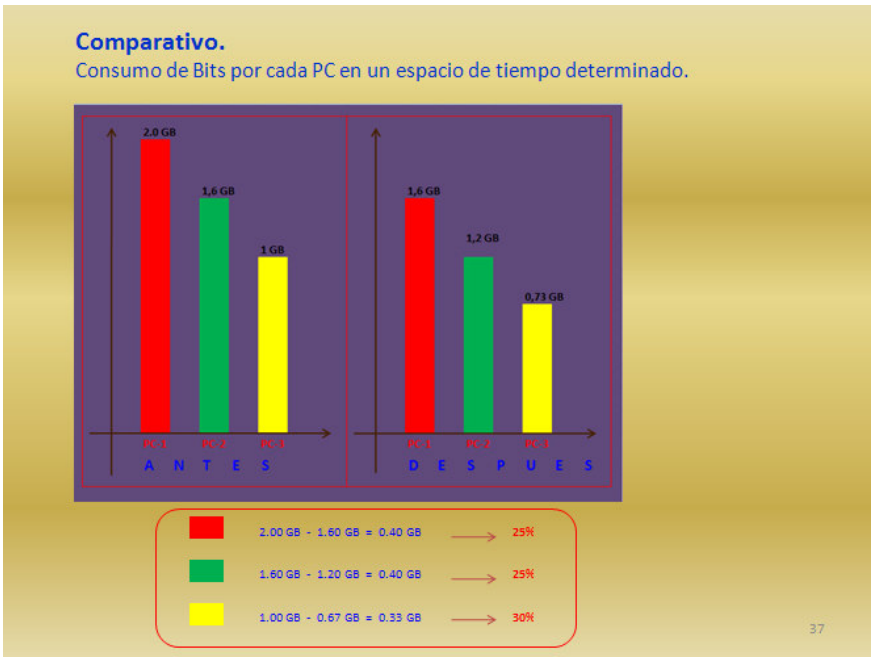
No.	Time	Client (IP:PORT)	URL	Length	Status
0	Jul 12, 14:06:37	10.0.0.3 :3539	http://www.google.com.pe/url?sa=t&rct=j&q=inabif&source=web&cd=1&sqi=2&ved=0CC0QFjAA&url=http%3A%2F%2Fwww.inabif.gob.pe%2F&ei=dFLgUffdLvOo4AOp8IHwDg&usg=AFQjCNEa6qNVCHg-U90FTH5kngRZjq6W8g&bvm=bv.48705608,d.dmg	254	200, FIN
1	Jul 12, 14:06:37	10.0.0.3 :3540	http://www.inabif.gob.pe/		302, FIN
2	Jul 12, 14:06:37	10.0.0.3 :3541	http://www.inabif.gob.pe/portalweb/index.php	18239	200, FIN
3	Jul 12, 14:06:37	10.0.0.3 :3546	http://www.youtube.com/embed/5Z7DxMrACE8	2143	200, FIN
4	Jul 12, 14:06:39	10.0.0.3 :3499	http://i1.ytimg.com/vi/5Z7DxMrACE8/hqdefault.jpg	16380	200, FIN
5	Jul 12, 14:06:41	10.0.0.3 :3584	http://spoc-pool-gtm.norton.com/register?t=600		Requested
6	Jul 12, 14:06:41	10.0.0.3 :3588	http://apps.shared.certified-toolbar.com/active.htm	1091	200, FIN
7	Jul 12, 14:06:44	10.0.0.3 :3539	http://www.google.com.pe/url?sa=t&rct=j&q=el%20comercio&source=web&cd=1&sqi=2&ved=0CC0QFjAA&url=http%3A%2F%2Felcomercio.pe%2F&ei=g1LgUYbKEZK24APgsoDIDA&usg=AFQjCNGKp0JkcGjrAUT2ZqQshpxJ9nZoQ&bvm=bv.48705608,d.dmg	250	200, FIN
8	Jul 12, 14:06:44	10.0.0.3 :3589	http://elcomercio.pe/	26375	200, FIN
9	Jul 12, 14:06:44	10.0.0.3 :3590	http://code2.adtlgc.com/js/comercio_init.js		304, FIN

Last update: Friday, July 12, 2013 14:10:36

4FUENTE: Elaboración propia

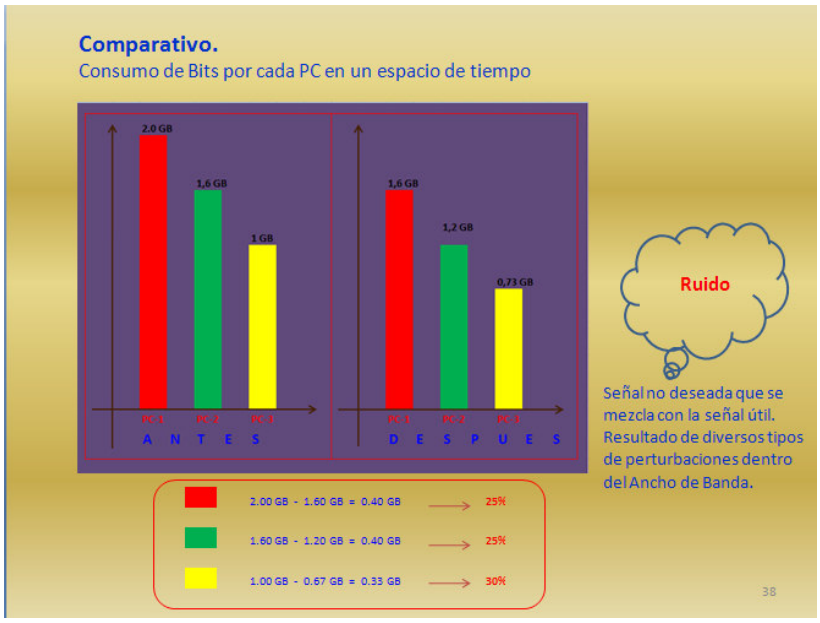
COMPARATIVO DE CONSUMO DE MEMORIA.

Figura: Comparativo de Consumo de memoria



FUENTE: Elaboración propia

Figura Comparativo de Consumo de memoria



FUENTE: Elaboración propia